

# LANDesk® Server Manager 8.6

## User's Guide



# Contents

Overview .....	1
About LANDesk® Server Manager .....	1
New to Version 8.6 .....	1
Product features .....	2
Getting started .....	3
Overview .....	3
Running the installation program .....	4
Activating the core server .....	4
Adding users .....	5
Configuring services and credentials .....	6
Running the console .....	7
Discovering devices .....	7
Scheduling and running the discovery .....	8
Viewing discovered devices .....	9
Moving devices to the My devices list .....	10
Grouping devices for actions .....	11
Configuring devices for management .....	11
Running the dashboard .....	12
Licensing .....	13
Adding licenses .....	13
The console .....	15
Starting the console .....	15
About the Server Manager login dialog .....	15
Using the console .....	15
My devices list .....	16
Device icons .....	18
Using shortcut menus .....	18
Using tools .....	18
Viewing device properties .....	19
Targeting devices .....	20
Filtering the display list .....	21
Using groups .....	21
Group types .....	22
Using the Actions tab .....	23

## TABLE OF CONTENTS

Delete devices.....	23
Power options .....	24
Assign attributes .....	24
Device monitor.....	24
Custom columns.....	25
Custom attributes .....	26
Page settings .....	26
Viewing the Server information console.....	27
Summary .....	27
Remote session .....	28
System information .....	28
Monitoring .....	29
Alert configuration .....	29
Vulnerabilities .....	30
Power options .....	30
Managing Intel® AMT devices .....	31
Intel AMT event log.....	32
Intel AMT power options .....	32
Forcing a vulnerability scan and disabling network access on Intel AMT machines .....	34
Opening the Intel AMT Configuration Screen.....	35
The dashboard.....	37
Using the dashboard .....	37
Configuring dashboard options.....	39
Role-based administration .....	41
About role-based administration .....	41
Understanding rights.....	42
Adding product users .....	47
Creating scopes.....	48
Default scopes .....	48
Custom scopes.....	49
Assigning rights and scope to users .....	49
About the User rights/scopes dialog .....	50
Device discovery .....	53
Using device discovery .....	53
Creating discovery configurations.....	54

Scheduling and running discovery .....	55
Viewing discovered devices .....	57
Adding categories .....	57
Moving discovered devices to the My devices list .....	58
Discovering Intel® AMT devices.....	58
Device agent installation and configuration .....	61
Agent installation and configuration overview .....	61
Updating existing agents .....	61
Uninstalling agents .....	62
Configuring agents.....	62
Deploying agents to managed devices .....	65
Configuring device authentication credentials .....	66
Installing agents.....	66
Installing agents.....	66
Uninstalling agents .....	67
Installing agents with an installation package .....	67
Pulling the agents .....	67
Understanding SERVERCONFIG.EXE .....	67
Creating an agent configuration.....	69
Pulling a Linux agent configuration.....	69
Creating standalone agent configuration packages.....	70
Pushing an agent configuration to devices .....	70
Installing Linux server agents.....	70
Deploying the Linux agents .....	71
Inventory scanner command-line parameters .....	72
Linux inventory scanner files .....	73
Console integration .....	73
Device monitoring .....	75
About monitoring.....	75
Deploying the monitoring agent to devices .....	76
Creating a monitoring configuration .....	76
Turning off the ModemView service .....	77
Setting performance counters.....	77
Monitoring performance.....	78
Monitoring configuration changes.....	79
Monitoring for connectivity.....	80

## TABLE OF CONTENTS

Alert configuration .....	83
Using alerts .....	83
How do I see alerts? .....	83
What kinds of device problems can generate alerts? .....	83
Configuring severity levels for events .....	84
Configuring alerts .....	85
Configuring alert actions .....	86
Configuring an alert ruleset .....	87
Deploying configurations .....	88
Viewing alert configurations for a device .....	89
Viewing the alert log .....	89
Vulnerability scanner .....	91
Vulnerability scanning overview .....	91
Understanding and using the Scan Vulnerabilities window .....	92
Configuring devices for vulnerability scanning .....	94
Updating vulnerability definitions .....	95
Scheduling vulnerability downloads .....	96
Viewing vulnerability and detection rule information .....	97
Purging vulnerability information .....	97
Scanning devices for vulnerabilities .....	98
Viewing detected vulnerabilities .....	99
Downloading patches .....	99
Remediating vulnerabilities .....	100
Remote server access .....	103
About remote access .....	103
Remote controlling devices .....	103
Using remote control .....	103
Configuring Windows 2003 client security for remote control .....	104
Controlling remote Windows devices .....	105
Viewing connection messages .....	105
Saving connection messages .....	106
Executing programs remotely .....	106
Transferring files to remote devices .....	106
Shutting down and rebooting remote devices .....	107
Configuring session options .....	107
Mirror driver .....	108

Accessing remote Linux devices .....	108
Software distribution .....	109
Software distribution overview.....	109
Using the Start command in a batch file package .....	110
Setting up a distribution package delivery server .....	111
Configuring Windows Web servers for software distribution.....	111
Configuring a network server for software distribution .....	113
Distributing software to Linux devices.....	114
Distribution file descriptions .....	115
File descriptions .....	115
About Distribution packages .....	117
Understanding the distribution package types.....	117
Resetting package hashes.....	118
Cloning .....	118
About the Scheduled tasks tab.....	118
About the Delivery methods tab.....	119
Understanding distribution error codes.....	120
Troubleshooting distribution failures .....	122
Scheduled task can't find package.....	123
Bandwidth detection doesn't work .....	123
Scripting.....	124
Scripting overview .....	124
Script commands.....	124
Editing packages with the Package Builder .....	124
Using scripting commands .....	125
Creating and naming software distribution packages.....	125
Simple sample script.....	126
Sample script with more complex commands.....	127
Package Builder .....	129
Running the Package Builder wizard .....	129
Setting up a package-building computer .....	130
Building a package.....	131
1. Taking a pre-installation snapshot .....	131
2. Installing the application or making a computer configuration change.....	132
3. Taking a post-installation snapshot.....	132
4. Restoring the package-building computer .....	133

## TABLE OF CONTENTS

Launching a package from a package .....	133
Using the Package Builder online help .....	133
Modifying the registry .....	133
OS deployment .....	135
OS deployment overview .....	135
OS deployment steps .....	136
OS image guidelines .....	136
Image filenames .....	136
Image file specifications and requirements .....	137
LANDesk agents and images .....	137
Partitions and images .....	137
Non-Windows images .....	137
Linux image specifications and requirements .....	137
Customizing images with Setup Manager and Sysprep .....	138
Creating a Sysprep image .....	139
For more information on Setup Manager and Sysprep .....	139
Creating imaging scripts with the OS Deployment wizard .....	139
Modifying scripts .....	140
Viewing image status reports .....	142
PXE-based deployment .....	142
PXE protocol basics .....	143
Using PXE representatives .....	143
Deploying PXE representatives .....	143
Booting devices with PXE .....	145
Understanding the PXE boot options .....	146
Configuring the PXE boot prompt .....	146
Using LANDesk managed boot .....	147
Using the PXE boot menu .....	147
Using the PXE holding queue .....	148
To schedule an OS deployment task .....	149
To add devices to the holding queue .....	149
Scheduling tasks .....	151
Scheduling tasks .....	151
Reports .....	155
About reports .....	155
Understanding report groups and predefined reports .....	155

Viewing reports .....	155
About the Report view window .....	155
Queries .....	157
Using queries .....	157
Queries overview .....	157
Query groups .....	157
Creating database queries .....	157
Running queries .....	160
Importing and exporting queries .....	160
Understanding custom queries .....	161
Creating custom queries .....	161
Managing queries .....	161
Step 1: Creating a search condition (required) .....	162
Step 2: Selecting attributes to display (required) .....	162
Step 3: Sorting results by attribute (optional) .....	163
Step 4: Running the query .....	164
Viewing query results .....	164
Viewing drill-down query results .....	164
Exporting query results to CSV files .....	165
Changing query column headings .....	165
Exporting and importing queries .....	165
LDAP queries .....	166
Inventory management .....	167
Managing inventory .....	167
Inventory scanning overview .....	167
Viewing inventory data .....	168
Viewing summary inventory from the local console .....	169
Viewing a full inventory .....	170
Viewing attribute properties .....	170
System information .....	170
Customizing inventory options .....	170
Editing the LDAPPL3.TEMPLATE file .....	171
Updating the application list .....	172
Publishing the application list .....	172
Software licenses .....	175
Monitoring software license compliance .....	175



## TABLE OF CONTENTS

How software license monitoring works.....	175
Software license compliance tree .....	176
Creating product and vendor aliases .....	176
Monitoring products for compliance .....	177
Setting up a product .....	177
Managing product groups.....	178
Managing products .....	178
Managing denied products .....	179
Selecting product files .....	179
Tracking licenses using the match all files option.....	180
Adding product license information.....	181
Denying product execution.....	182
Resetting usage data .....	182
Publishing the application list.....	183
Core database installation and maintenance.....	185
Installing an SQL or Oracle database .....	185
Microsoft SQL Server 2000 configuration .....	185
SQL maintenance .....	186
Oracle database configuration.....	187
Oracle performance tuning suggestions and scripts.....	187
Miscellaneous Oracle issues.....	187
Using rollup databases .....	189
Increasing the rollup database timeout .....	191
Configuring rollup database links.....	192
Oracle rolling to Oracle .....	192
SQL Server rolling to SQL Server .....	193
SQL Server rolling to Oracle .....	193
Oracle rolling to SQL Server .....	196
Multi-core support .....	197
Configuring COM+ server credentials.....	197
Appendices, copyright, and build information .....	199
Appendix A: System requirements and port usage.....	199
Administrative Core .....	199
Server Support (agents) .....	199
Browsers .....	199
Databases .....	200

Microsoft Data Access Components .....	200
Port usage .....	200
Ports used .....	201
Appendix B: Activating the core server .....	202
Appendix C: Configuring services .....	204
Selecting a core server and database .....	205
Configuring the Inventory service .....	205
Configuring duplicate device name handling .....	206
Configuring duplicate device ID handling .....	206
Configuring the scheduler service .....	207
Configuring the custom jobs service .....	209
Configuring the multicast service .....	210
Configuring the OS deployment service .....	210
Configuring the BMC password .....	211
Configuring the Intel AMT password .....	211
Appendix D: Agent security and trusted certificates .....	212
Backing up and restoring certificate/private key files among core servers .....	212
Appendix E: Additional OS deployment procedures .....	213
Additional OS deployment procedures .....	214
Adding application package distributions to the end of an OSD script .....	214
Using CSVIMPORT.EXE to import inventory data .....	214
Creating custom computer names .....	215
Customizing the SYSPREP.INF [RunOnce] section with tokenized inventory values .....	216
Using images in mixed uniprocessor and multiprocessor environments .....	216
Using the LANDesk imaging tool for DOS .....	217
Using the LANDesk imaging tool for Windows .....	219
Appendix F: IPMI support .....	222
Management features for IPMI-enabled devices .....	223
Appendix G: Intel® AMT support .....	224
Intel AMT provisioning requirements .....	224
Troubleshooting tips .....	225
Copyright and trademark notice .....	229



# Overview

---

## About LANDesk® Server Manager

Welcome to LANDesk® Server Manager 8.6, a stand-alone product that lets you maintain the availability of your servers—including those running Windows, Linux, HP-UX and AIX. It can also be installed and used concurrently with LANDesk Management Suite, using the same core database as Management Suite to ease IT-wide reporting.

Designed with an emphasis on low resource impact, this product has several "on-demand" agents and services that run only when they are needed, thus freeing memory and CPU cycles for other tasks. LANDesk knows device availability is critical for your company, so the product is designed for stability, running in 24/7 environments. It leaves you in control of the software running on your devices -- you can install the full agent, select specific components, or move devices to your device list without installing any agents.

### New to Version 8.6

**Expanded operating system support:** Manage your diverse server environment from one integrated console. In addition to managing Windows 2000 and 2003 servers, Server Manager provides support for several flavors of Linux and Unix:

- Red Hat Linux 9
- Red Hat Enterprise Linux AS, ES, and WS, version 3
- SUSE Linux Professional, ES, and AS, version 9
- HP-UX 11.1
- IBM AIX.

**OS deployment:** Operating System Deployment uses PXE-based deployment to deploy OS images to devices on your network, allowing you to automate many provisioning or repurposing tasks. OSD allows you to image devices with empty hard drives or unusable OSes using lightweight PXE representatives that eliminate the need for dedicated PXE servers on each subnet.

**Software licenses:** Inventory the software being used to assist you in implementing complete, effective software asset management and license compliance policies.

**Scheduled task view:** View all scheduled or completed agent deployment, vulnerability, software distribution, discovery, OSD, and custom script tasks from one location. You can reschedule the task, modify it, or make it a recurring event.

**Intel® AMT support:** Support for Intel's Active Management Technology. AMT is the ability to remotely manage networked devices in any system state through out-of-band (OOB) communication, even when the OS is unresponsive or the device is turned off. The only requirements on the device side are that it be connected to a corporate network and have stand-by power.

**Scripting tool:** You can execute custom tasks on devices. You can create OS and file deployment scripts.

## Product features

LANDesk® Server Manager enables you to choose your level of management coverage, from simple information gathering to extended performance analysis, security and configuration control. Server Manager includes the following:

**Easy-to-use Web console:** Run the product anytime, anywhere using a Web-based console designed to deliver rich data in an easy-to-use interface. You can run it from your primary workstation or from a workstation in the server room with no install. Simply browse to the product URL, <http://coreserver/LDSM>. "Target" specific devices for actions such as software distribution by selecting them for placement in the Targeted device list, similar to the "shopping cart" model in many Web applications.

**Dashboard:** The dashboard provides a quick real-time assessment of your managed devices. You can tell in an instant if any devices configured with the LANDesk monitoring agent have reached a Critical threshold on a given measurement, such as disk space or memory usage. The dashboard indicates how many devices are at each different status, and you can right-click a device to see a summary of its current condition or launch troubleshooting tools such as ping, trace route, or remote control. Double-click a device's icon to open its summary page.

**Performance monitoring:** You can monitor the real-time performance of your managed enterprise or blade servers, using a wide range of attributes. You can even track these attributes and see historical performance data reported over several days. You can monitor devices that have the monitoring agent installed, and you can also monitor out-of-band IPMI-enabled servers without an agent.

**On-demand management:** On-demand services that can be started only when you need them or during off-peak hours, thus freeing server bandwidth and resources for other uses. These services include remote control, inventory, software distribution, and vulnerability scanning.

**IPMI support:** The product provides support for Intelligent Platform Management Interface (IPMI) enabled servers (versions 1.5 or 2.0), allowing out-of-band remote recovery of downed servers and viewing of autonomous management data even when the OS or processor isn't running.

**Blade server support:** IBM blade chassis and server blades are supported, including discovery, chassis detection, inventory, software distribution and patch management capabilities. Product tools enable you to group blades by function, chassis, rack or other criteria for more effective data-gathering.

**Remote control:** You can remotely troubleshoot and resolve problems on Windows servers via application layer ring 3 remote control, providing increased stability over driver-level remote control solutions. For Linux machines, you can get quick remote access via SSH or SFTP. Remote control uses your own keyboard layout, so if you are using a Spanish language keyboard and need to remote to a device in the France office, your keystrokes will be "translated" to the French keyboard layout.

**Reporting:** You can run reports on any device in the database showing usage statistics, resource allocation, and many other measurements. This product includes several canned (pre-formulated) reports. These reports run quickly by directly accessing the database to gather information and represent data in two- or three-dimensional pie and bar graphs. You can create additional reports by creating custom queries.

**Health monitoring / Alerts:** Monitoring the overall health of a device is easy. You can set thresholds for measurements such as disk space or CPU usage, and configure how you want to be alerted in the event a threshold is exceeded. You can see health concerns of the selected device and initiate action to resolve the problem before users experience sluggish performance or downtime because of the problem.

**Vulnerability scanning and patch management:** You can receive automated vulnerability updates from industry sources such as Microsoft, as well as user-created custom vulnerability definitions, vulnerability detection and assessment. You can manually deploy the desired, tested patches using the software distribution capabilities.

**Software distribution:** Software distribution enables you to deploy a variety of software and file packages to Linux and Windows devices at your convenience. You can send a software package immediately or schedule it for off-peak hours.

**Role-based administration:** Add users and configure their access to tools and other devices based on their administrative role. With role-based administration, you assign scope to determine the devices a user can view and manage, and rights to determine the tasks they can perform, such as reporting only users.

**Inventory:** Using the inventory scanning tool, the product compiles a wealth of hardware and software information into the core database. You can then view, print, and export this data.

**Device discovery:** Be sure of what is on your network. Device discovery gathers basic information on all devices and other devices in your environment, enabling greater control and speeding agent deployment to targeted devices.

**Help:** This product includes a [Getting Started Guide](#), as well as context-sensitive help topics. Tutorials are available on the Web at <http://www.LANDesk.com/tutorials>.

## Getting started

---

- [Overview](#)
- [Running the installation program](#)
- [Activating the core server](#)
- [Adding users](#)
- [Configuring services and credentials](#)
- [Running the console](#)
- [Discovering devices](#)
- [Scheduling and running the discovery](#)
- [Viewing discovered devices](#)
- [Moving devices to the My devices list](#)
- [Grouping devices for actions](#)
- [Configuring devices for management](#)
- [Running the dashboard](#)

## Overview

Welcome to LANDesk® System Manager. LANDesk® Server Manager, a stand-alone device management application that maximizes your valuable time by letting you quickly and efficiently manage your devices. System Manager Server Manager lets you view your devices in a central location, group them for actions (such as power

cycling, vulnerability assessments, or configuring alerts), remotely troubleshoot any problems, and keep your devices updated with the latest patches.

This guide's purpose is to help you start using System ManagerServer Manager quickly by configuring services, running the console, discovering devices, moving the devices into the Managed list, and configuring the managed devices for actions.

System ManagerServer Manager is a Web application, allowing you to access it using your browser so you can manage your servers from a remote workstation. It behaves like many of the Web applications which you are accustomed to, but it also contains several advanced Windows-type controls to enhance your usability experience. For example, hover the mouse pointer over a control then double-click it or right-click it (just as you would in a Windows application). For example, in the **My devices** list, you can double-click a device name to access its specific information, or right-click to see available actions.

The steps below guide you through getting System ManagerServer Manager up and running, discovering devices on your network, selecting the servers to move to your **My devices** list, deploying agents, and then targeting those devices for various tasks.

## Running the installation program

During the install, on the Autorun page, select LANDesk System ManagerServer Manager.

After you have installed System ManagerServer Manager, you are ready to start using it. The sections below tell you how to complete several required tasks: running the core activation utility, configuring services, discovering computers, specifying which devices to actively manage by moving the devices the **My devices** list, grouping devices, adding users, and deploying agents.

## Activating the core server

Use the Core Server Activation utility to:

- Activate a new System ManagerServer Manager core server for the first time
- Update an existing System ManagerServer Manager core server or switch from a trial-use license to a full-use license

Each core server must have a unique authorization certificate.

With your core server connected to the Internet,

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Type in the unique user name and password provided by LANDesk when you purchased your licenses.
3. Click **Activate**.

The core communicates with the LANDesk Software licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require any intervention by you.

Periodically, the core server generates node count verification information in the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the LANDesk Software licensing server. This file is in XML format and is digitally signed and encrypted. Any changes made manually to this file will invalidate the contents and the next usage report to the LANDesk Software licensing server.

- The Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.
- You can also activate the core server by e-mail. Send the file with the .SAVE extension located under Program Files\LANDesk\Authorization to [licensing@landesk.com](mailto:licensing@landesk.com). LANDesk customer support will reply to the e-mail with a file and instructions on copying the file to the core server to complete the activation process.

## Adding users

System ManagerServer Manager users are users who can log in to the console and perform specific tasks for specific devices on the network. When you install the product, two user accounts are automatically created (see below). If you want to add more users, you can do so manually.

Users are not actually created in the console. Instead, users appear in the Users group (click **Users** in the left navigation pane) after they have been added to the LANDesk Management Suite group in the Windows NT users environment on the core server. The Users group shows all of the users currently residing in the LANDesk Management Suite group on the core server.

There are two default users in the Users group:

**Default Template User**—This user contains a template of user properties (rights and scope) that is used to configure new users when they are added to the Management Suite group. In other words, when you add a user to that group in the Windows NT environment, the user inherits the rights and scope currently defined in the Default Template User properties. If the Default Template User has all rights selected and the Default All Machines Scope selected, any new user placed in the LANDesk Management Suite group will be added to the Users group with rights to all of the product tools and access to all devices.

You can change the property settings for the Default Template User by selecting it and clicking **Edit**. For example, if you want to add a large number of users at once, but do not want them to have access to all of the tools or devices, change the settings for the Default Template User first, then add the users to the LANDesk Management Suite group (see steps below).

The Default Template User cannot be removed.

**Default Administrator**—This is the administrative user who was logged in to the server when System ManagerServer Manager was installed.

When you add a user to the LANDesk Management Suite group in Windows NT, the user is automatically read into the Users group in the **Users** window, inheriting the same rights and scope as the current Default Template User. The user's name, scope, and rights are displayed. Additionally, new user subgroups, named by the user's unique login ID, are created in the User Devices, User Queries, User Reports, and User Scripts groups (note that ONLY an Administrator can view User groups).



Conversely, if you remove a user from the LANDesk Management Suite group, the user no longer appears in the **Users** list. The user's account still exists on the core server and can be added back to LANDesk Management Suite group at any time. Also, the user's subgroups under User Devices, User Queries, User Reports, and User Scripts are preserved so that you can restore the user without losing their data, and so that you can copy data to other users.

Refresh the frame by pressing F5.

### To add a user or domain group to the LANDesk Management Suite group

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Groups | Groups** utility.
2. Right-click the LANDesk Management Suite group, and then click **Add to group**.
3. Click **Add**, then type or select a user (or users) from the list.
4. Click **Add**, and then **OK**.

**Note:** You can also add a user to the LANDesk Management Suite group by right-clicking the user account in the **Users** list, clicking **Properties | Member Of**, and then clicking **Add** to select the group and add the user.

If user accounts do not already exist on the server, you must first create them on the server.

### To create a new user account

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Group | Users** utility.
2. Right-click **Users**, and then click **New User**.
3. In the **New User** dialog, enter a name and password.
4. Specify password settings.
5. Click **Create**. The **New User** dialog remains open so that you can create additional users.
6. Click **Close** to exit the dialog.

Add the user to the LANDesk Management Suite group to have them appear in the **Users** group in the console.

## Configuring services and credentials

Before you can manage devices on your network, you must provide System ManagerServer Manager with the necessary credentials. Use the Configure Services utility on the core (SVCCFG.EXE) to specify the required operating system, Intel\* AMT, and IPMI BMC credentials. You can also specify additional settings, such as inventory defaults, PXE holding queue settings, and LANDesk database settings.

Use Configure Services to configure:

- The database name, username, and password. (Set at installation time.)
- Credentials for scheduling jobs to the managed devices. (You can enter more than one set of administrator credentials.)
- Credentials for configuring IPMI BMCs. (You can enter only one set of BMC credentials.)

- Credentials for configuring Intel AMT-enabled devices. (You can enter only one set of Intel AMT credentials.)
  - Server software scan interval, maintenance, days to keep inventory scans, and login history length.
  - Duplicate device ID handling.
  - Scheduler configuration, including scheduled job and query evaluation intervals.
  - Custom job configuration, including remote execute timeout.
1. At the core server, click **Start | All Programs | LANDesk | LANDesk Configure Services**.
  2. Click the **Scheduler** tab.
  3. Click the **Change Login** button.
  4. Enter the credentials you want the service to use on the managed devices, typically a domain administrator account.
  5. Click **Add**. Add additional credentials as necessary, if the managed devices do not all have the same administrator user name accounts enabled.
  6. Click **Apply**.
  7. If you have IPMI-enabled servers in your environment, click the **BMC Password** tab. Type a password in the **Password** text box, retype the password in the **Confirm password** text box, then click **OK**. (All managed IPMI servers must share the same BMC user name and password.)
  8. If you have Intel AMT-enabled devices, click the **Intel AMT Password** tab. Type the currently configured Intel AMT user name in the **User name** text box and the currently configured password in the **Password** text box. Retype the password in the **Confirm password** text box, then click **OK**.
  9. Set any other settings as desired, such as software scan intervals.
  10. Click **OK** to save the changes.

Click **Help** on each Configure Services tab for more information.

## Running the console

System ManagerServer Manager includes a full range of tools that let you view, configure, manage, and protect the devices on your network. The convenience of the console is that you can perform all of its functions from a remote location, such as your workstation - freeing you from the need to take additional trips to the server room or to go to each managed device individually to perform routine maintenance or troubleshoot problems.

Launch the console one of three ways:

- On the core server, click **Start | All Programs | LANDesk | System ManagerServer Manager**.
- In a browser at a remote workstation, type the URL *http://coreserver/LDSM*.
- In the dashboard, click **LDSM console**.

## Discovering devices

Use the Discovery Configuration dialog box to customize a scan to find unmanaged devices on your network. Use this dialog to isolate subnets or types of devices to reduce network traffic or the time required to complete the discovery task.

1. In the left navigation pane, click **Device discovery**.
2. On the **Discovery configurations** tab, click **New**.
3. Fill in the fields described below. When you are finished, click **OK**.

The text below describes the parts of the **Discovery configuration** dialog box.

- **Configuration name:** Type a name for this configuration.
- **Network scan (recommended):** Looks for devices by sending ICMP packets to IP addresses in the range you specify. By default, this option uses NetBIOS to try and gather information about the device.
  - The network scan option also has an **IP fingerprinting** option, where device discovery tries to discover the OS type through TCP packet responses. The IP fingerprinting option returns the most thorough information available, but it can take longer to complete.
- **LANDesk CBA:** Looks for the standard LANDesk agent (formerly known as the common base agent, CBA, in Management Suite) on devices.
- **IPMI:** Looks for IPMI-enabled servers. Intelligent Platform Management Interface (IPMI) is a specification developed by Intel, \* H-P, \* NEC, \* and Dell \* to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that let you access many features regardless of whether the system is turned on or not, or what state the OS may be in.
- **Chassis:** Looks for blade server chassis using the IBM/Intel architecture. The blade servers themselves are discovered using a standard network scan.
- **Intel\* AMT:** Looks for devices with Intel\* Active Management Technology-enabled devices installed. AMT is a platform-resident hardware and firmware solution that uses out-of-band communication to allow remote management regardless of the state of the operating system or platform power.
- **Starting IP:** Enter the starting IP address for the range of addresses you want to scan.
- **Ending IP:** Enter the ending IP address for the range of addresses you want to scan.
- **Subnet mask:** Enter the subnet mask for the IP address range you're scanning.
- **Add:** Adds your IP address range to the work queue at the bottom of the dialog.
- **Clear:** Removes the IP addresses and subnet mask from the text boxes.
- **Remove/Remove All:** Clears IP address ranges from the queue.

Now that you have configured a discovery, you can discover the devices connected to your network.

## Scheduling and running the discovery

Use the **Schedule** button on the **Discover devices** tab to display the **Schedule discovery** dialog. Use this dialog to schedule when a discovery or a deployment will run. You can schedule a discovery or client configuration to run immediately, at

some point in the future, make it a recurring schedule, or run it just once and never worry about doing it again.

Once you schedule a discovery or deployment, see the **Discovery tasks** tab for discovery status. Scheduling a recurring discovery assists you by automatically discovering new devices that come up on the network

The **Schedule discovery** dialog has these options.

- **Leave unscheduled:** Leaves the task unscheduled but keeps it in the **Discovery configurations** list for future use.
- **Start now:** Runs the task as soon as possible. It may take up to a minute for the task to start.
- **Start later:** Starts the task at the time you specify. If you click this option, you must enter the following:
  - **Time:** The time you want the task to start
  - **Date:** The date you want the task to start. Depending on your locale, the date order will be day-month-year or month-day-year.
  - **Repeat every:** If you want the task to repeat, select whether you want it to repeat **Daily**, **Weekly**, or **Monthly**. If you pick Monthly and the date doesn't exist in all months (for example, 31), the task will only run in months that have that date.

### To schedule a discovery

1. In the left navigation pane, click **Discovered devices**.
2. On the **Discovery configurations** tab, select the configuration you want and click **Schedule**. Configure the discovery schedule and click **Save**.
3. Monitor the discovery progress in the **Discovery tasks** tab. Click **Refresh** to update the status.
4. When the discovery completes, click **Unmanaged** to view all discovered devices in the upper **Discovered devices** pane (the pane does not refresh automatically).

## Viewing discovered devices

Discovered devices are categorized by device type in the **Discovered devices** pane. The **Computers** folder is displayed by default. Click the folders in the left pane to view devices in different categories. Click **Unmanaged** to view all devices returned by the discovery.

- Intel AMT-enabled devices appear in the **Intel AMT** folder.
- Blade chassis servers appear in the **Chassis** folder.
- Standard enterprise devices appear in the **Computers** folder.
- Routers and other devices appear in the **Infrastructure** folder.
- IPMI-enabled servers appear in the **IPMI** folder.
- Non-categorized devices appear in the **Other** folder.
- Printers appear in the **Printers** folder.

**Note:** Some Linux servers appear with the generic "Unix" as the operating system name (or even sometimes show as Other). When the standard LANDesk agent is deployed, these servers will update their OS name entry in the **My devices** list and display a full inventory.

### To view discovered servers

1. In the **Device discovery** page, in the left pane, click **Computers** or another type of device you want to view. The results are displayed in the right pane.
2. To filter the results, click the Filter icon, type at least a portion of what you are searching for, and click **Find**.

### Assigning names

When doing a network scan discovery, some servers return with blank node name (or host name). This occurs most frequently with servers running Linux. You must assign a name to the device before you can use Manage to move it to the My devices list.

1. In the **Device discovery** page, click the device with a blank name. (You must click the blank area in the node name column.)
2. Click **Assign name** on the toolbar.
3. Type in the name and click **OK**.

When you install a product agent on a device, it automatically scans the host name and updates the core database with the correct information.

### Moving devices to the My devices list

Once discovered, you must manually target the devices you wish to manage and move them to the **My devices** list. Moving the device does not install any software to the device. It only makes the device available for querying, grouping, and sorting in the **My devices** list.

1. In the **Discovered devices** view, click the device you want to move to the **My devices** list. You can select multiple devices by pressing SHIFT+click or CTRL+ click.
2. Click the **Target** button. If it is not visible, click << on the toolbar. The button is on the far right. Or, right-click the selected servers and click **Target**.
3. Click the **Manage** tab.
4. Select to move selected devices to the management database or select to move targeted devices.
5. Click **Move**.

Clicking **Move** moves the servers to the **My devices** list and places the device's information to the database. Once the information is in the database, you can run limited queries and reports on it (such as by device name, IP address or OS).

---

**Note:** If you choose to install the product agents manually by building them into a server image or by pulling the agency from the core server's LDLogon share, the devices automatically appear in the **My devices** list. You will not have to discover the devices and explicitly move them to the **My devices** list.

---

## Grouping devices for actions

You may want to organize your devices into groups, such as by geographic location or function, so you can perform actions on them more quickly. For example, you may want to see the processor speeds of all the servers in a specific location.

1. In the **My devices** list, click **Private groups** or **Public groups**, then click **Add group**.
2. Type a name for the group in the **Group name** box.
3. Click the type of group you want to create.
  - **Static**—Devices that have been added to the group. They remain in the group until they are removed or until you no longer manage them.
  - **Dynamic**—Devices that meet one or more criteria as defined by a query. For example, a group may contain all servers that are currently in a Warning state. They remain in the group as long as they match the criteria defined for the group.

To associate a query with a group, create the group, then click **My devices**, click **Public groups** or **Private groups**, click the group, then under Properties, click **Create a filter based on an existing query**. Select the query, then click **Create filter**.

4. When you are finished, click **OK**.
5. To add devices to a static group, click devices in the right pane of the **My devices** list, click **Move/Copy**, select the group, and click **OK**.

Devices are automatically added to dynamic groups when they meet the group query criteria.

## Configuring devices for management

Before you can fully manage devices with the console and receive health alerts, you need to install System ManagerServer Manager management agents on them. You can choose to install the default agent configuration (which installs all LANDesk agents) or customize your own agent configuration to install on your devices. (The agent configuration must include the monitoring agent to receive health alerts.)

To install management agents:

- Target devices in the **My devices** list, then schedule an agent configuration task to remotely install agents on the devices.
- Map to the core's LDlogon share (`\\coreserver\ldlogon`) and run `SERVERCONFIG.EXE`.
- Create a self-extracting device installation package. Run this package locally on the device to install the agents. This must be done while logged in with administrative privileges.

**To pull the agent from the LDlogon share (only works on Windows devices):**

1. At the system you want to configure, click **Start > Run**, then type `\\coreserver\ldlogon\ServerConfig.exe`.

2. Select the components you want to configure the system with, then click **Install**.
3. Follow the on-screen instructions.

The system now has the selected System ManagerServer Manager agents installed. No reboot is required. The server is automatically added to the **My devices** list.

### To push the agent:

1. Target devices in the **My devices** list (as explained above in Moving devices to the My devices list)
2. In the left navigation pane, click **Agent configuration**, right-click the configuration you want to push, and click **Schedule task**.
3. In the left pane, click **Target devices**, and click the **Add target list** button.
4. Click **Schedule task**, click **Start now** to start the task immediately or **Start later** and set the task's start date and time, and click **Save**.

You can view the status of the task in the **Configuration tasks** tab.

## Running the dashboard

The dashboard is a simple, high-level, uncluttered view of your devices. It represents each device with an icon whose color represents the device's current health. The dashboard also provides quick access to key troubleshooting tools.

To launch the dashboard:

- On the core server, click **Start | All Programs | LANDesk | System ManagerServer Manager Dashboard**.
- In a browser at a remote workstation, type the URL *[http://coreserver/LDSM/db\\_frameset.asp](http://coreserver/LDSM/db_frameset.asp)*.
- In the console, click **Dashboard**.

# Licensing

---

The license process helps keep your organization in compliance with its licensed node agreements by running an ongoing authorization process. This approach also enables you to use multiple core servers under a defined user account. The license process uses a backend database to create and manage user accounts. The license process is a simple request and reply from the core server to the backend process allowing the core to renew its activity for another period.

When you run the product (or any add-on) after an installation, you can choose Evaluation for a trial period or enter a username and password to activate a purchased license obtained from LANDesk Sales. A single username and password is used on all core servers for the existing account.

The activation process is essentially the same for evaluation and purchase products. When the device has an internet connection, the process is a simple information exchange. When the device is not connected, the manual process of e-mailing a file to LANDesk and then saving a returning file to the core server must be followed. The activation process works like this:

1. User runs [Activate Core utility](#)
2. A file is created containing both server and usage information, that is signed by the core's private key and encrypted with the LANDesk public key.
3. If an internet connection is available, the core and LANDesk servers communicate and uploads the activation file. The backend process the information and sends back the activation information which is written directly to the database.
4. If an Internet connection is not available, you may e-mail the file in Program Files/LANDesk/authorization file/ to [licensing@LANDesk.com](mailto:licensing@LANDesk.com).

## Adding licenses

The functionality available to you through the console is dependent on a license key. You can add a new license key to access additional functionality or update the number of users. During installation, a temporary 30-day license is generated. When you add a valid license in the console, the temporary license is deleted.

### To add a license key

1. In the left navigation pane, click **Preferences**.
2. Click the **License** tab.
3. At the bottom of the screen, click the link <http://www.LANDesk.com/contactus/>.

If the above link does not work, it could be because the browser Security level is not set to Medium. You should change the default Internet Security Level to **Medium** in Internet Explorer (Tools > Internet Options > Security > click the Internet icon > Default Level).





# The console

## Starting the console

### To start the console

1. On the core server, click **Start | Program Files | LANDesk | LANDesk Server Manager**.

*or*

On a remote workstation, open a browser and type the address of the console. This will be in the format of `http://corename/ldsm`

2. Enter a valid user name and password.

If you're connecting to a remote core server, follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).

3. Click **OK**.

---

If the device list and buttons do not appear when you start the console, you may need to [activate the core server](#).

---

## About the Server Manager login dialog

Use this dialog to launch the console and connect to a core server.

- **Username**—Identifies a user. This might be an administrator user or some other type of product user with restricted access (for more information, see [Role-based administration](#)). The user must be a member of the Server Manager group on the core server. If you're connecting to a remote core server, enter the user name/domain.
- **Password**—The user's password.

## Using the console

- [My devices list](#)
- [Public groups](#)
- [Private groups](#)

You can use tools to view, configure, manage, and protect the devices on your network—all from a single console. You can distribute and update software or configuration settings, diagnose hardware and software issues, use role-based administration to control users' access to features and devices, and use remote control features to train users or resolve problems. Additionally, if you are also using other LANDesk products, you can connect to them directly from the console. The System Manager help is available at <http://www.LANDesk.com/Support/Downloads/>.

The top pane in the console displays the server you are logged in to and the user you are logged in as. The **My devices** list is the main window of the console and is the starting point for most functions. The left-hand pane shows available tools. The right-hand pane in the console displays dialogs and screens which allow you to manage devices and users, view reports, run discoveries, create and modify queries, and so on. You can resize the panes and columns of the **My devices** list. When no agents are installed on a device, the name and IP address are the only columns that contain information. In some instances, the operating system will also display.

---

### Role-based administration

As a user, the devices you can view and manage in the **My devices** list and the management tools you can use are determined by the access rights and device scope assigned to you by the Administrator. For more information, see [Role-based administration](#).

---

This section provides information about:

- [My devices list](#)
- [Device icons](#)
- [Using shortcut menus](#)
- [Using tools](#)
- [Viewing device properties](#)

## My devices list

The **My devices** list contains the following groups and sub-groups. In addition, depending on your access rights and device scope, you can [create your own groups](#) for easier management of devices.

### All devices

The **All devices** list shows the devices for the currently logged-in user, based on the user's scope, in a flat list (no sub-groups). When connected to a particular core server, the administrator can see every device managed by that core server. Product users, on the other hand, are restricted and can only see the devices that reside within their assigned scope (a scope is based on either a database query or a directory location).

Devices running product agents (Standard LANDesk agent and Inventory) automatically appear in the **All devices** list when they are scanned into the core database by the inventory scanner. Typically, this scan takes place for the first time during initial device configuration. Once a device is scanned into the core database it is considered to be a managed device—it can now be managed by that core server. For more information on setting up devices, see [Configuring client agents](#).

Because the **All devices** group is populated automatically via an inventory scan, you may never need to manually discover devices. However, to discover devices not already in the core database (or to move unmanaged devices to the servers group), you can use the device discovery tool to scan the network for servers. For more information, see [Using discovery](#).

The **All devices** group provides the following information for each device. Double-click **All devices** to open the list.

- **Name:** The device host name, such as the Windows\* computer name.
- **IP address:** The IP address of the device.
- **Health:** The health and availability status of the device. This can be Normal, Warning, or Critical.
- **Agent:** The current agent running on the device.
- **Device type:** Displays the kind of hardware on the machine (AMT, IPMI, ASIC, or IPMI Advanced).
- **Operating system:** The type of operating system the device is running.
- **Up since:** The date and time the computer has been operating without interruption (in the time zone of the database).

When you select a device, the device's properties are displayed in the **Properties** pane below the device list. The **Properties** pane shows many important device attributes:

- **ID:** The identification number of the device. This number is determined by the sequence in which the device was added to the All devices list.
- **IP address:** The IP address of the device.
- **Manufacturer:** The device's manufacturer.
- **Model:** The model of the device.
- **Processor speed:** The speed of the device's CPU.
- **Processor type:** The type of the device's CPU.

From the console, you can remote control the machine, view a detailed inventory, assign attributes (such as Owner), and target the machine for an action, such as running a report. If the machine is a Linux server, you can use SSH and SFTP for remote access.

Double-clicking a device in the **All devices** list takes you to the [Server information console](#), which contains device summary information, configuration, remote control options, and alert configuration information.

## Public groups

The **Public groups** list shows groups of devices that have been created by a user with Administrator rights. They are visible to other users.

This list also shows blade chassis groups that are automatically created when a chassis management module (CMM) is added to the list of managed devices. The group lists the CMM and each associated blade server that you manage. You cannot edit a chassis group in the same way you edit a group you have created.

Groups can be static or dynamic. Dynamic groups contain devices that meet predefined filter criteria, such as processor speed, server OS, or a custom attribute such as a device type. Static groups include a set list of devices, other static groups, or dynamic groups.





## Private groups

The **Private groups** list shows groups of devices created by the currently logged-in user. Private groups are not visible to other users, so they can't be used by other users.

## Device icons

Device icons display in the **All devices** list and the [dashboard](#) and show the current health status of each device. You can update the health status for servers one at a time as you select them in devices in the **My devices** list by clicking the **Refresh** toolbar button.

The following table lists the possible device and status icons and what they mean:

Icon	Description
	Server with Normal status
	Server with Warning status
	Server with Critical status
	Server with Unknown status

---

### Icon display quality

These are high-color icons and require at least a 16-bit color-depth setting. If the icons in your console appear out of focus, change your color settings in the Windows Display Properties.

---

## Using shortcut menus

Shortcut (context) menus are available for all items in the console, including groups, devices, queries, scheduled tasks, scripts, and so on. Shortcut menus provide quick access to an item's common tasks and critical information.

To view an item's shortcut menu, right-click the item. For example, when you right-click a managed device in the **My devices** list, its shortcut menu will typically display the following options:

- **Remove from group:** Removes the item from a user-defined group.
- **Target:** Moves the selected device to the [Targeted devices](#) list.
- **Ping device:** Verifies the server is awake.
- **Tracert device:** Sends a trace route command to view a network packet being sent and received and the amount of hops required for the packet to reach its destination.
- **Remote control:** Launches the remote control window, allowing direct access to the selected server from the console.

The help does not cover every console item's shortcut menu, but it is recommended that you right-click any item to see the options that are available.

## Using tools

Tools are available through the left pane.

An administrator sees all of the tools in the left navigation pane. Other users will see only the tools (features) that are allowed by their assigned rights. For example, if a user doesn't have the Reports right, the Reports tool does not appear in the left navigation pane.

Here is a complete list of tools:

- **Agent configuration:** Configure an IPMI (Baseboard Management Controller), Linux, or Windows agent configuration.
- **Alerting:** Configure alerts, setting thresholds and the response the product will use if a threshold should be exceeded.
- **Dashboard:** Start the dashboard, a stand-alone utility that lets you see a quick view of the health of your devices.
- **Device discovery:** Find devices on the network that aren't scanned into the core database.
- **Directory manager:** Lets you locate, access, and manage devices in other directories via LDAP (the Lightweight Directory Access Protocol).
- **Distribution:** Distribute software packages, use custom scripts, schedule distributions, and create software distribution tasks.
- **Logs:** Displays the Alert log, which shows the alerts you have flagged as ones you want to see on your managed devices.
- **Monitoring:** Monitor the real-time performance of your managed devices using a wide range of attributes.
- **OS deployment:** Streamline new device provisioning without requiring additional end user or IT interaction once the process starts.
- **Queries:** Create and modify queries to the database to isolate specific devices that meet your criteria.
- **Remote control:** Remotely control devices and exchange files with them.
- **Reports:** Manage predefined service reports.
- **Scheduled tasks:** View all tasks (originating in Agent configuration, Vulnerabilities, Distribution, Device discovery, Scripts, or OS deployment) in the Scheduler.
- **Scripts:** Create and manage scripts.
- **Software licenses:** Provides the tools to implement complete, effective software asset management and license compliance policies.
- **Users:** Control user access to tools and devices based on user rights and scope.
- **Vulnerabilities:** Maintain patch-level security across the network by automating the repetitive processes of maintaining current vulnerability information.
- **Preferences:** Create custom inventory attributes and view licensing information.

When you click a tool name, the tool's window opens in the right pane.

## Viewing device properties

In the **My devices** view, you can quickly view information about a device by clicking the device in the list and selecting **Properties** in the bottom pane.

More detailed information about the device is available in its inventory data. You can view inventory data in the **All devices** view by clicking the device and selecting the **View inventory** tab in the bottom pane to open the full **Inventory** window.

### About the Properties screen

Use the Properties screen to view useful information about the selected server. The screen includes four buttons: **View details**, **View inventory**, **Assign attributes**, **Remote control**, **SSH**, and **SFTP**. Click each one to view related information.

### View details

Click this button to open the summary of the local console. The local console allows you to view detailed information about the device. You can also view current alert settings and launch troubleshooting tools such as remote control.

### View inventory

This button displays the full inventory of the selected server in a tree view.

### Assign attributes

Assigns custom attributes, such as location or owner, to the selected device. These [attributes must be created](#) in advance in **Preferences**.

### Remote control

Launches the remote control window, allowing direct access to the selected server from the console.

### SSH

Provides secure access to the selected Linux server. If the selected server is not a Linux server, this option is dimmed.

### SFTP

Provides secure FTP access to the selected Linux server. If the selected server is not a Linux server, this option is dimmed.

## Targeting devices

The **Targeted devices** list enables you to complete numerous tasks on selected devices, such as deploying agents or distributing software to a select group of devices.

The recommended number of devices that you should add to the list is 250 or fewer. The devices will stay in the list until your console session times out (after 20 minutes of inactivity).

Add devices to the **Targeted devices** list by using **Find computer** at the top of the My devices, Device discovery, and Queries console pages. Search for one particular device, or search for several using the wildcard characters of % or \*. Click the **Target** toolbar button to add the device to the **Targeted devices** list. If the button is not visible, click the << button.

If several devices are found, select the ones you want to add to the list, then click **Target**. If the returned device list spans multiple pages, you must click **Target computers** for each page. You can't select devices on multiple pages and click the buttons just once for all of the pages. You can click the down arrow below the toolbar

on the far right to set how many devices you want to display per page. You can display up to 500 devices per page.

In either case, the targeted devices will appear in the **Targeted devices** list.

With one or more devices in the **Targeted devices** list, you can complete many actions on them, such as distributing software or deploying agent configurations to the targeted devices via the software distribution wizard. All the devices in the **Targeted devices** list will receive the software package, eliminating the need for a query.

### To target devices


1. In the **My devices** list or the **Discovered devices** view, click the device you want to target for an action. You can select multiple devices by using the standard methods of multiple selection (SHIFT+click or CTRL+ click).
2. Click the **Target** button. If it is not visible, click << on the toolbar. The button is on the far right.

The selected devices are listed under the **Targeted devices** tab. Once they are listed under this tab, you can perform various actions on them, like add them to the database, reboot or turn them on and off, and so on.

## Filtering the display list

The **My devices** list has a filter icon you can use to determine which devices appear in the list. You can filter by only one of the criteria (by device name or IP address), or you can combine the criteria to focus on a subset of computers.

### To filter the display list

1. From the **My devices** list, double-click **All devices** or navigate to a group.
2. Click **Filter**  on the toolbar.
3. In the drop-down list, select **Device name** or **IP address**.
4. Set the parameters of the specified criteria by typing in the text box. In the **Find** box, the following extended characters are not supported: < , > , ' , " , !.

If you filter by device name, type the host name or range of computer names. You can enter wildcard characters to find certain computer names (such as \*srv).

5. Click **Find**.

## Using groups

You can organize computers in groups for easier management. You can create groups to organize devices based on function, geographic location, department, device attribute or any other category that meets your needs. For example, you could create a Web server group for all servers configured as Web servers, or create a group that includes all devices running a specific OS. You can right-click a group to



open it, delete it, or target all of the devices it contains for actions such as software distribution, alert configuration, and inventory scanning.

The main **My devices** view contains the following groups:

- **All devices:** Lists all devices that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). For an administrator, **All devices** lists all devices that have been scanned or moved into the core database. Devices configured with the standard LANDesk agent automatically appear in the **All devices** group/folder when they are scanned into the core database by the inventory scanner. Users, including administrators, cannot create groups under **All devices**.
- **Public groups:** Lists groups/devices an administrator has added from the **All devices** group, as well as blade chassis groups. An administrator (a user with the LANDesk administrator right) sees all of the devices in this group, while other users see only the devices allowed by their scope. Only administrators can create groups under **Public groups**.
- **Private groups:** Lists groups/devices for the currently logged-in user, based on the user's scope. A user can create device subgroups only under **Private groups**. Users can add devices to their **Private groups** group, or any of its subgroups, by moving or copying them from the **Public groups** and **All devices** groups. All users can create groups under **Private groups**.

---

For more information on which servers you can view and manage in the device view, and the management tools you can use, see [Role-based administration](#).

---

## Group types

You can create and manage two types of groups:

- **Static groups.** A *static group* is composed of devices that you have added manually to that group. Static groups can only be changed by manually adding or removing devices.
- **Dynamic groups.** A *dynamic group* is composed of computers that meet filter or query definition. Each time the group is expanded, the query is resolved and the results are displayed. For example, a dynamic group may contain all devices currently in a Warning state. Machines would move in and out of the group as their statuses change.

### To create a static group

1. In the console's device view, double-click the parent group (such as **Private groups**), and then click **Add group**.
2. Type a name for the new group.
3. Select **Static** and then click **OK**.

After you have created a static group, you can move/copy devices into the group by selecting them from the list and clicking **Move/copy** from the toolbar.

**To create a dynamic group**

1. In the console's device view, double-click the parent group (such as **Private groups**), and then click **Add group**.
2. Type a name for the new group.
3. Select **Dynamic** and then click **OK**.

After you have created a dynamic group, you must create a filter for it to determine which computers will appear in that group. You can specify a new filter or base the filter on an existing query.

**To create a new filter**

1. Select the dynamic group you created (this displays **Group properties** in the bottom pane).
2. From **Group properties**, select **Create a new filter** and click **Create filter**.
3. Select the filter criteria you want to use, then click **OK**.

**To create a filter based on an existing query**

1. Select the dynamic group you created (this displays **Group properties** in the bottom pane).
2. From **Group properties**, select **Create a filter based on an existing query**.
3. Select the existing query you want to use to filter the group and click **New filter**.
4. Add any additional filter criteria you want to use, then click **OK**.

---

If you base a filter on an existing query and that query is later modified by you or another user, the filter based on that query will not dynamically change to match the modified query.

---

## Using the Actions tab

Use the **Actions** tab to execute various operations on selected and targeted devices. You can delete devices from the list of managed computers, power on, power off, and reboot devices.

- [Delete devices](#)
- [Power options](#)
- [Assign attributes](#)
- [Device monitor](#)

## Delete devices

**Delete devices** lets you delete selected or targeted devices from the list of managed computers. The delete function can delete single or multiple devices from any group (either a default group or user-created group) in Server Manager. Once a device has been deleted from a group, it is completely removed from Server




Manager list of managed/inventoried devices, including the default **All devices** group.

If you are deleting a large number of devices, the operation may time out. If the operation times out, try breaking up the operation into smaller operations.

## Power options

**Power options** lets you power off, reboot and, in the case of managed IPMI machines, power on remote devices. In the case of non-IPMI servers, the device must have the LANDesk Server Manager agent deployed to it in order to execute the reboot and power off functions. With IPMI machines, you must have the correct IPMI credentials to execute the power on/power off and reboot features. If an IPMI box has the LANDesk Server Manager agent deployed to it, then you can execute the power off and reboot features without the IPMI credentials. Use SVCCFG.EXE to set the IPMI BMC password to use for managing IPMI servers.

### To use power options

1. In the **My devices** list, click a device or [target](#) a list of devices.
2. In the bottom pane, click the **Actions** tab.
3. Click **Power options**.
4. Select whether to perform the action on devices in the [Targeted devices](#) or only selected devices.
5. Select from the following options:
  -  Reboot
  -  Power off
  -  Power on (only works on IPMI-enabled machines)

## Assign attributes

Use **Assign attributes** to designate specific attributes for the selected device. For example, you can assign a location to the device. These attributes cannot be created in this view. They must be created in the [Custom attributes tab](#) under **Preferences**.

1. In the **All devices** list, click a device or [target](#) a list of devices.
2. In the bottom pane, click the **Actions** tab.
3. Click **Assign attributes**.
4. In the drop-down list for the attribute, select a value. Repeat as necessary.
5. Select whether to perform the action on devices in the [Targeted devices](#) or only selected devices.
6. Click **Assign**.

## Device monitor

Use **Device monitor** to check the connectivity of the selected devices. If a device loses its network connectivity, it cannot send an alert to the core server. Device monitor checks to see devices are still able to communicate on the network.

1. In the **All devices** list, click a device or [target](#) a list of devices.
2. In the bottom pane, click the **Actions** tab.
3. Click **Device monitor**.
4. Type numbers for the minutes between pings and number of retries.
5. Select whether to ping all devices, to ping only [targeted devices](#), or to never ping devices.
6. Click **Apply**.

## Custom columns

Use Custom columns to modify column names and fields. A Name is the name of the column, and a Field is the attribute(s) that can appear in the column (if the attribute is present). Any column changes you make will not be seen by other users. Custom column changes will be seen in the My devices view.

It is not advisable to create custom columns in which there can be multiple field names. For example, if you were to create a Computer.Software.Package.Name field and the server had multiple packages installed, Server Manager will list only one package name per line, even if the different package names are on the same device, making the All devices list and dashboard have multiple entries for the same device.

To change a column name

1. In the left navigation pane, click **Preferences**.
2. Click the **Custom columns** tab.
3. Click **Edit columns**.
4. In the top box, select a column heading and click **Add**.

The box shows a list that represents all of the inventory data currently in the database. Drill down this list to select an attribute to display in the query results list. Remember to select attributes that will help you identify the clients returned in the query. If you cannot find attributes you want to display, you can add them in the [Custom attributes](#) dialog. However, these attributes must be assigned to machines before they appear in the query dialog.

**Note:** If you're using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, and so on).

**Note:** If you select an attribute in the database that has a 1:\* relationship, you will get duplicate entries for the device. Attributes with a 1:1 relationship (only one possible attribute, like Computer.System.Asset Tag), you will not receive duplicate entries.

5. To replace an existing heading, select the heading in the lower box, click **Edit**, make your modifications, and press **Enter**. The following extended characters are not supported: < , > , ' , " , !.
6. To change the order of the columns, select a column heading and click **Move Up** or **Move Down**.

## Custom attributes

Attributes are characteristics or properties that belong to a device. The more attributes a device has in the database, the easier it becomes to uniquely identify the device. You can create custom attributes and assign those to a device or set of devices.

There are nine categories of non-inventoriable attributes to let you add custom data and associate it with specific devices. By explicitly listing the nine categories, this is modeled data, and now you can add that data as a custom column in the **My devices** view or run a query on that attribute.

The values you can add to that attribute however are dynamic and unlimited. For example, using the Location 1, 2 and 3 categories, you could enter values like assorted Country names in Location 1, Town names in Location 2, and Building names in Location 3. Then you could run a query to find a list of machines where Town name= London and you could then do something to that specific set of machines.

You must have the Administrator right to create custom attribute values.

### To create custom attribute values

1. In the left navigation pane, click **Preferences**.
2. Click the **Custom attributes** tab.
3. Double-click the attribute name for which you want to create a custom value.
4. Type the new value in the **Attribute: name** box, and click **Add Value**.
5. To add another value, erase the value in the **Attribute: name** box, type the new value, and click **Add Value**.
6. To remove a value, select the value and click **Remove**.
7. To change the order the values will appear in the **Attribute: name** drop-down list, select the value and click **MoveUp** or **MoveDown**.
8. To replace a value, select an existing value, type the replacement value in the **Attribute: name** box, and click **Replace**.
9. When finished, click **OK**.

### To assign custom attributes to devices

1. In the All devices list, click a device.
2. In the bottom pane, click the **Actions** tab.
3. Select **Assign attributes** from the left pane.
4. Each Attribute Name has a drop-down list of values. These values are created in Creating custom attributes above. Select a value from the drop-down list for the attribute name, and repeat as necessary.
5. Click **Targeted devices** or **Selected devices** to apply the attributes to those devices in the Target Devices list or those selected and highlighted in the My devices list, and click **Assign**.

## Page settings

Use **Page settings** to set display preferences for pages listing devices or displaying graphics.

1. In the left navigation pane, click **Preferences**.
2. Click the **Page settings** tab.
3. In the **Graph type** drop-down, select the type of graph you want to display in Reports.
4. In the **Items/page** box, type the maximum number of items you want to display in each page that uses pagination.
5. Click **Update**.

## Viewing the Server information console

Use the Server information console to view top-level summary information about a device, view system information like CPU or fan information, monitor the health status and thresholds of key components of a device, manage vulnerabilities, and power on, power off, or reboot a device. The Server information console has the following sections listed under the left navigation pane.

- [Summary](#)
- [Remote session](#)
- [System information](#)
- [Monitoring](#)
- [Alert configuration](#)
- [Vulnerabilities](#)
- [Power options](#)

### Summary

Use the **Summary** page to view important information about the selected device. It is located under **System information**.

#### To view a device's summary

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.

The console opens in another browser window. The **Summary** page is displayed by default. The information listed on the page includes:

- **Health:** The overall health of the device as defined by the conditions and parameters you set.
- **Type:** The type of the device, such as print, application, or database.
- **Manufacturer:** The maker of the device.
- **Model:** The model of the device.
- **BIOS version:** The version of the device's BIOS.
- **Operating system:** The device's operating system.
- **OS version:** The version number of the operating system.
- **CPU:** The manufacturer, model, and speed of the device's processor.
- **Vulnerability scanner:** The version of the vulnerability scanner.
- **Remote control:** The version of the remote control agent.
- **Software distribution:** The version of the software distribution agent.
- **Inventory scanner:** The version of the inventory scanner.

- **IPMI version:** The version of IPMI the device is using (if applicable).
- **CPU usage:** The percentage of the processor currently being used.
- **Physical memory used\*:** The percentage of total physical memory used on the device.
- **Virtual memory used\*:** The percentage of total virtual memory used on the device.
- **Last reboot\*:** The date and time the device was last rebooted (in the time zone of the database).
- **Drive:** The drives on the device with the total size of the drive and percentage of space used.

This information is pulled from the registry in Windows or from configuration files in Linux.

\*This information appears when an agent has been installed on the device.

## Remote session

Use **Remote session** to start a remote control session with the selected device. If the device is a Windows server, standard LANDesk remote control launches. For Linux servers, you can choose between SSH and SFTP remote sessions.

1. In the **My devices** view, double-click the device you want to configure.
2. In the left navigation pane, click **Remote session**.

## System information

Use **System information** to run detailed information about the selected device. Many reports are available from this page under the headings of Hardware, Software, Logs, and Other.

### To view information for an individual device

1. In the **My devices** view, click the device.
2. In the **Properties** page, click **View details**.

The console opens in a different browser window.

3. In the left navigation pane, click **System information**.
4. Click the information you would like to view.

Some inventory-related data fields in Hardware (like CPU) are in English only.

### To view information for a blade chassis management module (CMM)

1. In the **My devices** view, click the CMM.
2. In the **Properties** page, click **Launch CMM console**.

The console opens in a different browser window.

3. In the left navigation pane, click the information you would like to view.

## Monitoring

Use **Monitoring** to view performance counters and graphs, and to set thresholds for device components.

### To monitor devices

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.

The console opens in a different browser window.

3. In the left navigation pane, click **Monitoring**.
4. Select **Performance counter settings**.
5. From the **Objects** column, select the object you want to monitor.
6. From the **Instances** column, select the instance of the object you want to monitor, if applicable.
7. From the **Counters** column, select the specific counter you want to monitor.
8. Specify polling interval and days to keep history.
9. In the **Alert after counter is out of range** drop-down list, specify the number of times the counter will be allowed to cross the thresholds before an alert is generated.
10. Specify upper and/or lower thresholds.
11. Click **Apply**.

## Alert configuration

Use the **Alert configuration** page to view a list of the alert configurations assigned to the selected device, and to view the details of each alert.

### To view alert configurations

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.

The console opens in a different browser window.

3. In the left navigation pane, click **Alert configuration**.

The following text describes the details provided about each alert. For more information on modifying these details, see [Alerting](#).

- **When state reaches:** When the state of the alert reaches the displayed state, an alert will be generated.
- **Affects health:** If the alert state reaches the specified threshold, the state affects the overall health state of the device. The selection of an alert affecting health is determined in the Alert configuration dialog.
- **Ruleset name:** The name of the alert ruleset, as defined in the [Alert configurations](#) dialog.
- **Alert type:** The kind of alert to be generated, such as an e-mail, an SNMP trap, or executing a program.



- **Action configuration:** The action that occurs when the alert is generated, as defined in the [Action configurations](#) dialog.
- **Alert handler:** The handler associated with the alert, such as an e-mail handler.
- **Instance:** A number indicating how many times the alert can occur before an action is executed.

## Vulnerabilities

Use the **Vulnerabilities** page to scan for vulnerabilities on the selected device.

### To check device vulnerabilities

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.

The console opens in a different browser window.

3. In the left navigation pane, click **Vulnerabilities**.

### Column descriptions

- **ID:** Identifies the vulnerability with a unique, vendor-defined alphanumeric code.
- **Severity:** Indicates the severity level of the vulnerability. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown.
- **Title:** Describes the nature or target of the vulnerability in a brief text string.
- **Language:** Indicates the language of the OS affected by the vulnerability.
- **Date published:** Indicates the date the vulnerability was published by the vendor.
- **Silent install:** Indicates whether the vulnerability's associated patch file installs silently (without user interaction). Some vulnerabilities may have more than one patch. If any of a vulnerability's patches don't install silently, the vulnerability's **Silent install** attribute is **No**.
- **Repairable:** Indicates whether the vulnerability can be repaired through patch file deployment and installation. Possible values are: Yes, No, and Some (for a vulnerability that includes multiple detection rules and not all detected vulnerabilities can be repaired).

## Power options

**Power options** lets you power off, reboot and, in the case of managed IPMI and Intel AMT devices, power on remote devices. In the case of non-IPMI servers, the server must have the LANDesk Server Manager agent deployed to it in order to execute the reboot and power off functions.

With IPMI and Intel AMT devices, you must have configured the correct credentials to execute the power on/power off and reboot features. If IPMI or Intel AMT devices have the LANDesk Server Manager agent deployed, then you can execute the power off and reboot features without the IPMI or AMT credentials. To configure BMC credentials for IPMI devices, or Intel AMT device credentials, use the Configure Services utility (see [Configuring services and credentials](#)).

### To use power options on the selected device




1. In the **My devices** view, click the device you want to configure.

2. In the **Properties** page, click **View details**.

The console opens in a different browser window.

3. In the left navigation pane, click **Power options**.

4. Select from the following options:

-  Reboot
-  Power off
-  Power on

5. Click **OK**.

Additional options are available for properly configured IPMI and Intel AMT devices.

## Managing Intel® AMT devices

After an Intel AMT-configured device has been discovered and its user name/password configured, it can be managed in limited ways even if the device does not have a Server Manager agent installed.

The following table lists the management options available when a device has Intel AMT only compared with Intel AMT and a Server Manager agent.

	Intel AMT only	Intel AMT and agent	Agent only
Inventory	summary	X	X
Event log	X	X	X
Remote boot manager	X	X	
Disable OS network		X	
Enable OS network		X	
Force vulscan on reboot		X	
Inventory history		X	X
Remote control		X	X
Chat		X	X
File transfer		X	X
Remote execute		X	X
Wake up		X	X
Shut down		X	X
Reboot		X	X
Inventory scan		X	X
Scheduled tasks and policies	limited	X	X

Group options		X	X
Run inventory report		X	X
AMT alerting		X	X

#### To view the Intel AMT inventory summary for a device

1. Double-click the device in the **All devices** list.
2. In the server information console, click **Intel AMT options**.
3. Click **Inventory summary**.

The summary shows the device's GUID, product and manufacturer, serial number, and BIOS, processor, and memory summaries, and the Intel AMT version number. If any information is missing you can refresh the data by clicking **Update inventory**.

## Intel AMT event log

Server Manager provides a view of the event log that Intel AMT devices generate. The AMT settings determine what events are captured in this log. You can view the date/time of the event, the source of the event (Entity column), a description, and the severity as determined by the AMT settings (Critical or Non-Critical). You can also export the log data in comma-separated value (CSV) format.

#### To view the Intel AMT event log

1. Double-click the device in the **All devices** list.
2. In the server information console, click **System information**.
3. Click **Logs** to expand it, then click **Intel AMT log**.
4. To export the log to a CSV format file, click the **Export** button on the toolbar and specify a location to save the file to.
5. To clear all data in the log, click the **Purge log** button on the toolbar.
6. To update the log entries, click the **Refresh log** button on the toolbar.

## Intel AMT power options

This product contains options to power on and off Intel AMT devices. These options can be used even when a device's operating system is not responding, as long as the device is connected to the network and has standby power.

When Server Manager initiates power option commands, in some cases it is not possible to verify that the commands are supported on the hardware receiving the command. Some devices with Intel AMT may not support all power option features (for example, a device may support IDE-R reboot from CD but not from a floppy). Consult the hardware vendor's documentation if it appears that a power option is not working with a particular device.

You can simply turn on or off the device's power, or you can reboot and specify how the device is rebooted. The options are described in the table below.

Power off	Shuts down the power on the device
Power on	Turns on the power on the device

Reboot	Cycles the power off and on again on the device
Normal boot	Starts up the device using whatever boot sequence is set as the default on the device
Boot from local hard drive	Forces a boot from the device's hard drive regardless of the default boot mode on the device
Boot from local CD/DVD drive	Forces a boot from the device's CD or DVD drive regardless of the default boot mode on the device
PXE boot	When restarted, the PXE-enabled device searches for a PXE server on the network; if found, a PXE boot session is initiated on the device
IDE-R boot	Reboots the device using the IDE redirection option selected (see below)
Enter BIOS setup	When the device is booted, it allows the user to enter the BIOS setup
Show console redirection window	When the device is booted, it starts in serial over LAN mode to display a console redirection window
IDE redirection: Reboot from floppy	When the device is booted, it starts from the floppy disk drive or image that are specified (floppy image files must be in .img format; see note below)
IDE redirection: Reboot from CD/DVD	When the device is booted, it starts from the CD drive or image that are specified (CD image files must be in .iso format; see note below)
IDE redirection: Reboot from specified image file	When the device is booted, it starts from the image file that is specified (see note below)

### To use AMT power options

1. Double-click the device in the **All devices** list.
2. In the server information console, click **Power options**.
3. Select a power command. If you select **Reboot**, select a boot option.
4. Click **Send** to initiate the command.

### Notes on using IDE redirection options

To use IDE redirection options, both a boot floppy or floppy image file and a boot CD/DVD or CD/DVD image file must be specified. Floppy image files must be in .img format, and CD image files must be in .iso format. Some BIOSes may require the CD image to be located on a hard drive.

Intel AMT normally remembers the last IDE-R settings, but Server Manager clears the settings after 45 seconds, so on subsequent boots it will not restart the IDE-R feature. The IDE-R session on an Intel AMT device lasts 6 hours or until the Server Manager console is turned off. Any IDE-R operation still in progress after 6 hours will be terminated.

## Forcing a vulnerability scan and disabling network access on Intel AMT machines

When an Intel AMT-configured device has the Server Manager agent installed, the agent includes functionality that can help resolve problems with malicious software or other issues that prevent you from accessing the device.

The amtmon.exe service is installed with the Server Manager agent. When this service is running on a device, you can force a vulnerability scan at the next reboot to attempt to identify any malicious software on the device. If communication with the device fails, you can disable the device's network connection even if the OS is not functional, such as when malicious software has disabled the OS by consuming all CPU cycles. By disabling the network connection you can prevent the device from sending unwanted packets through the network.

When the Server Manager agent is installed on an Intel AMT device, the following options are available on the **Intel AMT options** page:

- **Operating system network connection:** click **Disable** to disable the OS network stack to stop network access; click **Enable** to enable OS network access if it has been disabled.
- **Scan for vulnerabilities after reboot:** forces the Server Manager vulnerability scanner to run the next time the device reboots.

When a device is not responding or may have malicious software running on it, the recommended use case is to first run a vulnerability scan on the next reboot to attempt to identify the problem. If the problem continues and the machine is infecting/attacking the network, or if you can't access the device, you have the option to disable the OS NIC.

### To force a vulnerability scan after a reboot

1. Double-click the device in the **All devices** list.
2. In the device console window, click **Intel AMT options**.
3. Click **Configuration options**, then click **Scan**. A message appears on the device stating that a scan will be run the next time it reboots.
4. To shut down or reboot the device, use the Intel AMT remote boot manager features above.

### To disable or enable the network connection on an unresponsive device

1. Double-click the device in the **All devices** list.
2. In the device console window, click **Intel AMT options**.
3. To disable the device's network card to stop communication with other devices on the network, click **Disable**. When the network connection is disabled, a message appears on the device stating that the network card has been disabled.
4. If the device is safe to connect to the network again, click **Enable**. When the connection is restored, a message appears on the device stating that the network card is enabled again.

## Opening the Intel AMT Configuration Screen

Server Manager includes a link that lets you open the Intel AMT Configuration Screen. This is an interface provided by Intel to view device status, hardware information, the AMT event log, remote boot settings, and network settings. It also lets you add and edit AMT user accounts for the device. The window that displays this screen is separate from the Server Manager console, and any questions you may have about your use of this interface should be to the device manufacturer's technical support.

### To open the Intel AMT Configuration Screen

1. Double-click the device in the **All devices** list.
2. In the device console window, click **Intel AMT options**.
3. Click **Intel AMT console**, then click **Launch Intel AMT web console**.



# The dashboard

---

## Using the dashboard

- [To open the dashboard](#)
- [To use the dashboard](#)
- [To view device properties](#)
- [To perform basic troubleshooting tasks](#)
- [To sort the dashboard](#)
- [To dock the dashboard window](#)
- [To view by criticality](#)
- [To refresh the dashboard](#)
- [To view the console](#)

The dashboard is a simple, high-level, uncluttered view of your devices. It represents each device with an icon that shows the device's current health. The devices viewed in the dashboard are based on scopes and roles. The dashboard is movable and configurable. The dashboard displays the overall health of all the devices in the view, listing the number of devices by state (X number of devices in Critical state, X number of devices in Normal state). You can view a graph and server list or undock the graph and view that by itself on your workstation or a group monitor.

When you right-click a device's icon, you can view device properties or a more detailed state of the device displayed in a pop-up window. From this window, you can view the type of the device, and the percentages of key resources used on the device. You can also select basic troubleshooting items, such as ping, trace route and remote control (if the device is managed), or double-click the icon to go to the console. The dashboard runs on the same [browsers](#) as the main product.

### To open the dashboard

1. In the left navigation pane, click **Dashboard**.

or

On the core server, click **Start | All programs | LANDesk | LANDesk Server Manager Dashboard**.

or

In a browser at a remote workstation, type the URL  
*[http://coreserver/LDSM/db\\_frameset.aspx](http://coreserver/LDSM/db_frameset.aspx).*

---

It is recommended that you open the dashboard soon after you install the core to verify that it is not a "blocked site." In Windows 2003, you may receive "site blocked" messages due to scripting and a Flash\* control that runs under the dashboard. If this occurs, make the following changes to security in Internet Explorer.

---

Internet Explorer security settings for Windows 2003:

1. Open Internet Explorer, and click **Tools | Internet Options | Security**.



2. Click **Trusted sites | Sites** and add *http://CoreName* to the list of trusted Web sites, then click **OK**.
3. In the same dialog (**Internet Options | Security**), click **Internet** and lower the Security level from High to Medium.
4. In the same dialog, click **Custom Level**; under "Scripting - Active scripting" select **Enable**, then click **OK**.

### To use the dashboard

1. To view a device's **Server information console**, double-click the device.

A device's Server information console page lists basic inventory, patch management, and system information,

### To view device properties

1. From the dashboard, right-click a device, then click **Properties**.

You can view the device name, IP address, the percentage of CPU and memory usage, and the amount of hard disk space remaining.

### To perform basic troubleshooting tasks

The dashboard provides basic troubleshooting functionality, such as pinging the device, remote control (if the device is managed), and access to a device's [server information console](#).

1. To remote-control a device, right-click the device and select **Remote control**.
2. To ping a device, right-click the device and select **Ping device**.
3. To send a trace route command to a device, right-click the device and select **Tracert device**.
4. To view the device's server information console, double-click the device.

### To sort the dashboard

1. In the dashboard toolbar, click the **Sort By** drop-down list, then select either **Name** or **Health**.

### To dock the dashboard window

1. In the dashboard toolbar, click **Dock graph**.

The dockable window opens in a new browser. To return to the dashboard, click the dashboard browser window.

### To view by criticality

1. In the dashboard toolbar, click the **View** drop-down list and select an option such as **Critical**.

or

Click a bar on the graph to view only servers matching that status.

#### To refresh the dashboard

1. In the dashboard toolbar, click **Refresh**.

This adds/removes devices and updates the status of each device.

#### To view the console

1. In the dashboard toolbar, click **LDSM console**.

This opens the console if it is not already opened. If the console is already open, it sets the focus to the console.

## Configuring dashboard options

The **Dashboard options** page lets you configure the way you want the dashboard to display.

1. In the left navigation pane, click **Dashboard**, then click **Options**.
2. Type a number (in seconds) in the **Update every** box to set how often you want the dashboard to check for health status updates.
3. Select the graph type you want to display from the **Graph type** list box (3D bar, 3D pie, 2D bar, 2D pie).
4. In the **View** list box, select the status category you want to display. You can display all devices, or display devices by status type (Unknown, Warning, Critical, Critical/Warning).
5. Select how you wanted the devices sorted (by Name or Health).
6. Click **Large icons** to display the dashboard view with large icons.
7. Click **List view** to list the devices with the same columns as the main console. **Large icons** do not apply to this view.
8. Click **OK**.



# Role-based administration

---

## About role-based administration

Use role-based administration to configure user access to product tools and other devices based on their administrative role in your system. With role-based administration, you assign scope to determine the devices a user can view and manage, and rights to determine the tasks they can perform.

Administrators (users with the LANDesk Administrator right) can access the role-based administration tools by clicking **Users** in the left navigation pane.

Role-based administration lets you assign product users special administrative roles based on their rights and scope. *Rights* determine the product tools and features a user can see and utilize. *Scope* determines the range of devices a user can see and manage.

You can create roles based on users' responsibilities, the management tasks you want them to be able to perform, and the devices you want them to be able to see, access, and manage. Access to devices can be restricted to a geographic location like a country, region, state, city or even a single office or department. Or, access can be restricted to a particular platform, processor type, or some other device hardware or software attribute. With role-based administration, it's completely up to you how many different roles you want to create, which users can act in those roles, and how big or small their scope of device access should be.

For example, you can have one or more users whose role is software distribution manager, another user who is responsible for remote control operations, a user who runs reports, and so on.

### Example administrative roles

The table below lists some of the possible administrative roles you might want to implement, the common tasks that user would perform, and the rights that user would need in order to function effectively in that role.

Role	Tasks	Required rights
Administrator	Configure core servers, manage users, configure alerts, integrate other company products, etc. (Of course, administrators with full rights can perform any management tasks.)	Administrator (all rights implied)
Asset manager	Discover devices, configure devices, run the inventory scanner, enable inventory history tracking, etc.	Unmanaged device discovery, software distribution, and public query management
Deployment manager	Create images, deploy OS images, deploy PXE representatives, assign PXE holding queues, configure the	OS deployment

	PXE boot menu, create boot floppy disks, etc.	
Helpdesk	Remotely control devices, chat, transfer files, execute software, shutdown, reboot, view agent and health status, etc.	Remote control, basic Web console
Application manager	Create software packages, scripts, and delivery methods, and distribute software packages.	Software distribution and configuration
Reporting manager	Run predefined reports, print reports, etc.	Reports (required for all reports)
Software license monitoring manager	Configure applications to monitor, add licenses, upgrade and downgrade licenses, verify reports, etc.	Software license monitoring

These are just example roles. Role-based administration is flexible enough to let you create as many custom roles as you need. You can assign the same few rights to different users but restrict their access to a limited set of devices with a narrow scope. Even an administrator can be restricted by scope, essentially making them an administrator over a specific geographic region or type of managed device. How you take advantage of role-based administration depends on your network and staffing resources, as well as your particular needs.

To implement and enforce role-based administration, simply designate current local Windows users, or create and add new local Windows users, as Server Manager users, add the users to the LANDesk Management Suite user group, and then assign the necessary rights (to product features) and scope (to managed devices). Follow the procedures below:

## Understanding rights

Rights provide access to specific tools and features. Users must have the necessary right (or rights) to perform corresponding tasks. For example, in order to remote control devices in their scope, a user must have the remote control right. Rights can be assigned to the user from either the Server Manager or Management Suite console, and are effective in both consoles.

When a right is not assigned to a user, tools associated with that right are not visible to that user in the product console. For example, if a user is not given the reports right, the reports item doesn't appear in the left navigation pane. The table below shows which rights are required for the tool to display for a user.

<b>Tool</b>	<b>Rights needed to display in left navigation pane</b>
My devices	Basic Web console
Agent configuration	Software distribution, Software distribution configuration, OS deployment
Alerting	Alerting/monitoring
Dashboard	Basic Web console
Device discovery	Discovery

Directory manager	Software distribution, Software distribution configuration, OS deployment
Distribution	Software distribution, Software distribution configuration, OS deployment
Monitoring	Alerting/monitoring
OS deployment	OS deployment
Queries	Basic Web console, Public queries, Reports
Reports	Reports, Software license monitoring, Patch, Patch compliance
Scheduled tasks	Discovery, Software distribution, Software distribution configuration, OS deployment, Patch, Patch compliance, Connection control manager
Scripts	Software distribution, Software distribution configuration, OS deployment, Patch, Patch compliance
Software assets	Software license monitoring
Users	Administrator
Vulnerabilities	Patch, Patch compliance
Preferences	Basic Web console

See the descriptions below to learn more about each product right and how rights can be used to create administrative roles.

---

### Scope controls access to devices

When using the features allowed by these rights, users will always be limited by their scope (the devices they can see and manipulate).

---

## LANDesk Administrator

The LANDesk Administrator right provides full access to all of the product tools (however, use of these tools is still limited to the devices included in the administrator's scope).

This is the default right for a newly added user, unless you've modified the settings for the Default Template User.

The LANDesk Administrator right provides users the ability to:

- See and access the **Users** tool in the left navigation pane
- See product licensing in **Preferences** in the left navigation pane.
- Perform all of the product tasks allowed by the other rights listed below

---

### Note on rights and tools

The LANDesk Administrator right is exclusively associated with the **Users** tool. If a user does not have the LANDesk Administrator right, this tool will not appear in the console.

All of the tools in the product console are associated with a corresponding right (as described below).

---

### Device discovery

The Device discovery right provides users the ability to:

- Find devices on the network that haven't submitted an inventory scan to the product core database through many ways, such as a network scan, Standard LANDesk agent discovery, and IPMI discovery
- Schedule periodic discoveries
- Move devices from Discovered to Managed

### OS deployment

The OS deployment right provides users the ability to:

- See and access the **Scripts** tool in the left navigation pane
- Create and run OS deployment scripts
- Schedule OS deployment tasks
- Configure PXE representatives with the Deploy PXE Representative script
- Designate PXE holding queues
- Configure the PXE boot menu

### Remote control

The remote control right provides users the ability to:

- Use the remote control options on a device's shortcut menu (otherwise, they are dimmed if the Basic Web console right is enabled)
- Remote control devices that have the remote control agent loaded
- Power up, shut down, and reboot devices (devices can only be powered up if they are IPMI devices)
- Chat with devices
- Execute device programs remotely
- Transfer files to and from devices

### Software distribution

The software distribution right is a subset of the Software distribution configuration right, and provides users the ability to:

- Create and run software distribution scripts
- Ability to view and use the directory manager
- Schedule other script-based tasks

### Public query management

The Public query management right provides users the ability to:

- Create queries available to all users
- Ability to create or delete public queries
- Ability to modify/edit existing public queries

## Reports

The reports right provides users the ability to:

- See and access the **Reports** tool in the left navigation pane
- Run predefined reports

## Patch manager

The Patch manager right is specific to the vulnerability scanning feature. For more information, see "[Using the vulnerability scanner](#)."

## Asset configuration

The Asset configuration right is an administration-level right that is only available if you have purchased LANDesk Asset Manager. It provides users the ability to:

- See and access all the asset management links in the console: Assets, Contracts, Invoices, Projects, Global lists, Detail templates, and Reports.
- Create new types
- Edit types (both predefined and custom)
- Delete types
- Create, edit, and delete subgroups used to organize types
- Create new details for types
- Edit details (both predefined and custom)
- Create and modify detail templates
- Create and modify detail tables
- Create, edit, and delete sections used to organize details
- Perform all of the Asset Manager tasks allowed by the other rights listed below

## Asset data entry

The Asset data entry right is only available if you have purchased LANDesk Asset Manager, and provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, and Global lists links in the console.
- Browse types and details (can't add, edit or delete them)
- Add items to the database by filling in data entry forms
- Edit items that have been added to the database

## Software license monitoring

The software license monitoring right provides users the ability to:

- See and access the **Software licenses** tool in the left navigation pane
- Configure applications to monitor, add licenses, upgrade and downgrade licenses, and verify reports.



### Software distribution configuration

The Software distribution configuration right is the primary distribution right. Users with this right can do everything available in software distribution.

- Create software packages
- Deploy packages to managed devices.

For more information, see "[Software distribution](#)."

### Connection control manager

The Connection control manager right is a Management Suite right that provides users with the ability to:

- See and access the **Connection control configuration** tool in the Management Suite Tools menu and Toolbox
- Control the access to external devices to control and configure them

### Patch compliance

The Patch compliance right provides users the ability to:

- Add and remove security definitions from the Compliance group
- Change the status of definitions contained in the Compliance group

Users with this right cannot edit custom definitions or security threat's custom variables.

### Basic Web console

The Basic Web console right provides users with the ability to use the features associated with the right. The features are listed below, along with any exceptions within the feature.

- My devices (the right doesn't allow for the updating of public groups, or deleting devices under the Actions tab)
- Change preferences (but not custom attributes)
- Dashboard

### Alerting and monitoring

The Alerting and monitoring right provides users with the ability to:

- Monitor the performance of various system and OS components, such as drives, processors, memory, processes, bytes/sec transferred by the system's Web server, and so forth
- Track the exact health of all managed devices

- Customize alerts to be sent by severity level (Critical, Warning, Informational, OK, Unknown) or threshold (for example, if the hard disk usage exceeds 90% of hard disk capacity)
- Choose the action to be taken if an alert exceeds a threshold (by adding information to the log, e-mailing a notice, running a program on the core or an individual device, or sending an SNMP trap to an SNMP management console on the network)

## Adding product users

Product users are users who can log in to the product console and perform specific tasks for specific devices on the network.

Product users are not actually created in the console. Instead, users appear in the **Users** tab (in the left navigation pane, click **Users**) after they have been added to the LANDesk Management Suite group in the Windows NT users environment on the core server. The **Users** group shows all of the users currently residing in the LANDesk Management Suite group on the core server.

There are two default users in the **Users** group:

- **Default Template User**—This user is basically a template of user properties (rights and scope) that is used to configure new users when they are added to the LANDesk Management Suite group. In other words, when you add a user to that group in the Windows NT environment, the user inherits the rights and scope currently defined in the Default Template User properties. If the Default Template User has all rights selected and the Default All Machines Scope selected, any new user placed in the LANDesk Management Suite group will be added to the **Users** group with rights to all of the product tools and access to all devices.

You can change the property settings for the Default Template User by right-clicking it and clicking **Edit rights**. For example, if you want to add a large number of users at once, but do not want them to have access to all of the tools or devices, change the settings for the Default Template User first, then add the users to the LANDesk Management Suite group (see steps below).

The Default Template User cannot be removed.

- **Default Administrator**—This is the administrative user who was logged in to the server when LANDesk Software core was installed.

When you add a user to the LANDesk Management Suite group in NT, the user is automatically read into the **All Users** group in the **Users** window, inheriting the same rights and scope as the current Default Template User. The user's name, scope, and rights are displayed.

If you remove a user from the LANDesk Management Suite group in the Windows users environment, the user is no longer an active LANDesk user and can be deleted from the **Users** group. The user's account still exists on your server and can be added back to LANDesk Management Suite group at any time. Also, the user's subgroups under **User Devices**, **User Queries**, **User Reports**, and **User Scripts** are preserved so that you can restore the user without losing their data, and so that you can copy data to other users.

To refresh the **Users** list to display any newly added users, click **Users** and click the **Refresh** button on your browser.

**To add a user or domain group to the LANDesk Management Suite group**

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Groups | Groups** utility.
2. Right-click the **LANDesk Management Suite** group, and then click **Add to group**.
3. Click **Add**, then type or select a user (or users) from the list.
4. Click **Add**, and then **OK**.

---

**Note:** You can also add a user to the LANDesk Management Suite group by right-clicking the user account in the Users list, clicking **Properties | Member Of**, and then clicking **Add** to select the group and add the user.

---

If user accounts do not already exist in NT, you must first create them on the server.

**To create a new user account**

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Group | Users** utility.
2. Right-click **Users**, and then click **New User**.
3. In the New User dialog, enter a name and password.
4. Specify password settings.
5. Click **Create**. The New User dialog remains open so that you can create additional users.
6. Click **Close** to exit the dialog.
7. Add the user to the LANDesk Management Suite group to have them appear in the Users group in the console.

You can now assign your product users rights and scope.

## Creating scopes

A scope defines the devices that can be viewed and managed by a product user. Scopes can be assigned to the user from either the Server Manager or Management Suite console, and are effective in both consoles.

A scope can be as large or small as you want, encompassing all of the managed devices scanned into a core database, just a single device, or no devices. This flexibility, combined with modularized tool access, is what makes role-based administration such a versatile management feature.

### Default scopes

Role-based administration includes two default scopes. These two predefined scopes can be useful when configuring the user properties of the default template user.

- **(Default) No Machines Scope:** Excludes all devices in the database.
- **(Default) All Machines Scope:** Includes all devices in the database.

You can't edit or remove the default scopes.

## Custom scopes

There are three types of custom scopes you can create and assign to users:

- **Query-based:** Controls access to only those servers that match a custom query search. You can select an existing query, or create new queries from the **Assign devices to users** dialog, to define a scope. Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group. For more information on creating queries, see "[Creating database queries](#)."
- **Group-based:** Controls access to only those devices located in the selected group. You can select groups from the **Group scope properties** dialog to define a scope.
- **LDAP- or custom directory-based:** Controls access to only those devices located in an Active Directory or NetWare eDirectory LDAP-compliant directory structure, or in a custom directory location. You can select directory locations when you click on the **New inventory scope** button.

You can assign more than one scope to any of the users. When multiple scopes are assigned to a user, the cumulative effective scope (i.e., the complete range of devices that can be accessed and managed as a result of the combination of assigned scopes) is a simple composite.

You can customize a user's effective scope by adding and removing scopes at any time. All types of scopes can be used together.

### To create a scope

1. In the left navigation pane, click **Users**.
2. Click the **Scopes** tab, and then click the **New query scope**, the **New group scope**, or the **New inventory scope** toolbar button.
3. Enter a name for the new scope.
4. If you selected query-based, choose an existing query, or click **Define** to create a new query. Click **OK**.
5. If you selected group-based, choose a group, then click **OK**.
6. If you selected inventory-based, choose a directory, then click **OK**.
7. Click **OK** to save the scope and close the dialog.

## Assigning rights and scope to users

Once you've added product users, learned about rights and how they control access to features and tools, and created device scopes to allow or restrict access to managed devices, the next step in establishing role-based administration is to assign the appropriate rights and a scope to each user.

You can modify a user's rights and scope at any time.

If you modify a user's rights or scope, those changes will take effect the next time that user logs into the console.

### To assign rights and scope to a user

1. In the left navigation pane, click **Users**.

2. Select the **Users** tab to view all of the users that are currently a member of the LANDesk Management Suite group in the core server's Windows NT environment.

The **Users** tab displays a list of users, including their user name and assigned rights (a check character indicates the right is enabled or active).

3. Right-click a user, and then click **Edit rights**.
4. In the **User rights/scope** dialog, check or clear rights as desired.
5. Select a scope from the **Available scopes** list.
6. Click **OK**.

The new rights display next to the user's name in the list and will take effect the next time the user connects to the core server.

### To delete a scope

1. In the left navigation pane, click **Users**.
2. In the **Scope** tab, click the scope you want to delete and click **Delete**. Click **OK**.

Exercise caution when deleting scopes. The users assigned to them will be able to access rights previously prohibited by the scope.

## About the User rights/scopes dialog

Use this dialog to view and modify a user's assigned rights and scope. Open the dialog by selecting a user and clicking **Edit rights**.

- **Rights tab:** Lists the rights assigned to the user.
  - **LANDesk Administrator**
  - **Device discovery**
  - **OS deployment**
  - **Remote control**
  - **Software distribution**
  - **Public query management**
  - **Reports**
  - **Patch manager**
  - **Asset configuration**
  - **Asset data entry**
  - **Software license monitoring**
  - **Software distribution configuration**
  - **Connection control manager**
  - **Patch compliance**
  - **Basic Web console**
  - **Alerting and monitoring**
- **Scope tab:** Lists the scopes assigned to the user.
  - **Assigned scopes:** Identifies the user's current scopes.
  - **Add:** Opens the **Add scope** dialog where you can select a scope to add to the user.
  - **Remove:** Deletes the selected scope.

- **Apply:** Saves your changes to the user's properties and closes the dialog.
- **Cancel:** Closes the dialog without saving changes.



# Device discovery

---

## Using device discovery

Device discovery finds devices on your network that do not have agents installed and have not submitted an inventory scan to the Server Manager core database. Device discovery has multiple ways of finding devices on your network.

- **Network scan:** Looks for computers by doing an ICMP ping sweep. This is the most thorough search, but it can take longer. You can limit the search to certain IP and subnet ranges. By default this option uses NetBIOS to gather information about the device. You can also select IP Fingerprinting, which also provides the OS type (in most cases).
- **CBA discovery:** Looks for the Standard LANDesk agent (formerly known as the common base agent [CBA] in Management Suite) on computers. This option discovers computers that have Server Manager, System Manager, and so on. You can click the option under Standard LANDesk agent discovery to discover devices using the older LANDesk PDS2 agent. CBA discovery is not supported for Linux machines, but if you choose PDS2, Linux machines with an agent installed can be discovered.
- **IPMI:** Looks for servers enabled with [Intelligent Platform Management Interface](#), which allows you to access many features regardless of whether the server is turned on or not, or what state the OS may be in.
- **Server chassis:** Looks for blade server chassis management modules (CMMs). The blades in the server chassis are detected as normal servers.
- **Intel\* AMT:** Looks for Intel Active Management Technology-enabled devices.

Device discovery tries to discover basic information about each device.

- **Node name:** The discovered device name, if available.
- **IP address:** The discovered IP address.
- **Subnet mask:** The discovered subnet mask.
- **Category:** The device discovery group the device belongs to.
- **OS name:** The discovered OS description, if available.

Depending on the device and the type of discovery selected, device discovery may not have information for all columns. When device discovery finds a device for the first time, it looks in the core database to see if that device's IP address and name are already in the database. If there's a match, device discovery ignores the device. If there isn't a match, device discovery adds the device to the **Unmanaged** device table. Devices in the **Unmanaged** table don't use a Server Manager license. A device is considered managed once it sends an inventory scan to the core database. Once you move a device to the **All devices** group, it no longer displays in the **Discovered devices** list.

IPMI devices must have a BMC (baseboard management controller) that is configured in order to be discovered as IPMI devices and to use full IPMI functionality. If the BMC is not configured, the device can be discovered as a computer. You can then add the device to the list of managed devices and run the Configure Services utility to configure the BMC password. The device's IPMI functionality will then be recognized by this product.



To automate device discovery, you can schedule discoveries to occur periodically. For example, you could divide your network by subnets and schedule a ping sweep for a different subnet each night. In all discoveries, the core server does the discovering.

To discover and manage devices on your network, complete the following tasks:

- Create discovery configurations
- Schedule and run the discovery
- View discovered devices
- Move discovered devices to the **My devices** list

---

### Unmanaged device discovery can't discover firewalled devices

Be aware that unmanaged device discovery usually can't discover devices that use a firewall, such as the Windows Firewall that is built into Windows XP. The firewall typically prevents the device from responding to the discovery methods that unmanaged device discovery uses.

---

## Creating discovery configurations

Use the **Discovery configurations** tab to create new discovery configurations, edit and delete existing configurations, and schedule a configuration for discovery. Each discovery configuration consists of a descriptive name, the IP ranges to scan, and the discovery type.

Once you create a configuration, use the **Schedule discovery** dialog to configure when it will run.

1. In the left navigation pane, click **Device discovery**.
2. In the **Discovery configurations** tab, click the **New** button.
3. Fill in the fields described below. When you are finished, click the **Add** button, and click **OK**.

The text below describes the parts of the **Discovery configuration** dialog box.

- **Configuration name:** Type a name for this configuration. Give the configuration a meaningful name so you can easily remember the configuration. The configuration can be up to 255 characters long, and should not contain the following characters: ", +, #, & or %. The configuration name will not display after the use of any of these characters.
- **Network scan:** Looks for devices by sending ICMP packets to IP addresses in the range you specify. This is the most thorough search, but also the slowest. By default, this option uses NetBIOS to gather information about the device.

The network scan option also has an **IP fingerprint** option where device discovery tries to discover the OS type through TCP packet responses. The IP fingerprint option slows down the discovery somewhat.

- **CBA discovery:** Looks for the standard LANDesk agent (formerly known as the common base agent [CBA] in Management Suite) on devices. The standard LANDesk agent allows the core server to discover and communicate with clients on the network. This option discovers devices that have Server Manager agents on them. Routers block standard LANDesk agent and PDS2 traffic. In order to run a standard CBA discovery across multiple subnets, the

router must be configured to allow directed broadcast across multiple subnets.

The CBA discovery option also has a **PDS2 discovery** option, where device discovery looks for the LANDesk Ping Discovery Service (PDS2) on devices. LANDesk Software products such as LANDesk® System Manager, Server Manager, and LANDesk Client Manager use the PDS2 agent. Select this option if you have devices on your network with these products installed. CBA discovery is not supported for Linux machines, but if you choose PDS2, Linux machines with with an agent installed can be discovered.

- **IPMI:** Looks for IPMI-enabled servers. IPMI is a specification developed by Intel,\* H-P,\* NEC,\* and Dell\* to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that let you access these features regardless of whether the device is turned on or not, or what state the OS may be in. Please keep in mind that if the Baseboard Management Controller is not configured, it will not respond to ASF pings which the product uses to discover IPMI. This means that you will have to discover it as a normal computer. When you push the client, ServerConfig will scan the system and detect it is IPMI and configure the BMC. For a brief overview of IPMI, see "[Appendix E: IPMI support](#)."
- **Server chassis:** Looks for blade server chassis management modules (CMMs). The blades in the server chassis are detected as normal servers.
- **Intel\* AMT:** Looks for devices with Intel Active Management Technology support.
- **Starting IP:** Enter the starting IP address for the range of addresses you want to scan.
- **Ending IP:** Enter the ending IP address for the range of addresses you want to scan.
- **Subnet mask:** Enter the subnet mask for the IP address range you want to scan.
- **Add:** Adds the IP address ranges to the work queue at the bottom of the dialog.
- **Clear:** Clears the IP address range fields.
- **Remove:** Removes the selected IP address range from the work queue.
- **Remove all:** Removes all IP address ranges from the work queue.

#### To edit or delete a configuration

- On the **Discovery configurations** tab, click the configuration you want and click **Edit** or **Delete**.

## Scheduling and running discovery

Use the **Schedule** button on the **Discovery configuration** tab to display the **Scheduled task** dialog. Use this dialog to schedule when discovery configurations run. You can schedule a discovery configuration to run immediately, run at some point in the future, make it a recurring schedule, or run it just once.

Discovery tasks can be rescheduled or deleted from the **Discovery tasks** tab. Once you schedule a discovery, see the **Discovery tasks** tab for discovery status. You can also access discovery task status from the **Scheduled tasks** tool. Once a discovery task completes, new devices not already in the core database will be added to the discovered device categories.

The **Schedule discovery** dialog has these options.

- **Leave unscheduled:** (default) Leaves the task in the Task list for future scheduling.
- **Start now:** Runs the task as soon as possible. It may take up to a minute for the task to start.
- **Start later:** Starts the task at the time you specify. If you click this option, you must enter the following:
  - **Time:** The time you want the task to start
  - **Date:** The date you want the task to start. Depending on your locale, the date order will be day-month-year or month-day-year.
  - **Repeat every:** If you want the task to repeat, select a frequency (every Day, Week, or Month). If you pick Month and the date doesn't exist in all months (for example, 31), the task will only run in months that have that date.

#### To schedule a discovery

1. In the left navigation pane, click **Device discovery**.
2. On the **Discovery configurations** tab, select the configuration you want and click **Schedule**. Configure the discovery schedule.
3. Monitor the discovery progress in the **Discovery tasks** tab.
4. When the discovery completes, view all discovery results in the upper **Discovered devices** pane.

The **Discovery tasks** tab shows discovery job status. The status includes the following:

- The discovery configuration's name.
- The task status, which can be Working, All Completed, None Completed, or Failed.
- The last time the task ran.
- The type of task run.

#### To delete or reschedule a discovery

If you want to delete a task from the list, whether it has run already or not, click the task and click **Delete**. If the task hasn't run yet or is a recurring task, deleting it prevents it from running in the future.

You can also reschedule a discovery task in the list to run again or at a different time by clicking the task and clicking **Reschedule**.

#### To view discovery task status

1. In the left navigation pane, click **Discovered devices**.
2. Click the **Discovery tasks** tab.

## Viewing discovered devices

When device discovery finds a device, it tries to identify the device type so it can add the device to one of these categories:

- **AMT:** Contains devices with Intel Active Management Technology support.
- **Chassis:** Contains blade server chassis management modules (CMMs).
- **Computers:** Contains computers. Linux systems may be labelled as Unix systems in the OS Name column.
- **Infrastructure:** Contains routers and other network hardware.
- **IPMI:** Contains IPMI-enabled devices.
- **Other:** Contains unidentified devices.
- **Printers:** Contains printers.

These seven categories help keep the **Device discovery** list organized so you can more easily find the devices you're interested in. You can sort the device lists by any column heading when you click on a heading. Device discovery may not categorize devices correctly every time. You can easily move misidentified devices to the correct group by right-clicking the device you want to move, clicking **Move**, selecting the correct category, then clicking **Move**.

### To view discovered devices on the network

1. In the **Device discovery** page, in the left pane, click **Computers** or another type of device you want to view. The results are displayed in the right pane.
2. To quickly locate a device or filter a list based on a specific criteria, click the filter toolbar button to expand the filter toolbar.
3. In the **Filter by** list, select the column you want to filter: **Node name**, **IP address**, **Subnet mask**, **Category**, or **OS name**. Enter the value you want to filter on, and click **Find**.

The filter may return devices with no node name in addition to the criteria you specify.

## Adding categories

You can create categories to further group discovered devices. If you move a device to another category, device discovery will leave that device in that category if device discovery detects the device again later. By keeping the main **Computers** category organized and by moving devices you know you won't be managing with Server Manager to other categories, you can easily see new devices in the **Computers** category. If you delete a category that contains devices, device discovery moves the devices to the **Other** category.

### Adding a device category

Use **Add category** to create a device category in the **Discover devices** view. Default categories are Computers, Printers, Infrastructure, and Other.

1. In the **Device discovery** view, click **Add category**.

2. Type a name for the group in the **Category name** box.
3. When you are finished, click **OK**.

## Moving discovered devices to the My devices list

1. In the **Discovered devices** view, click the device you want to move to the **My devices** list. You can select multiple devices by using the standard methods of multiple selection (SHIFT+click or CTRL+ click).
2. Click the **Target** button. If it is not visible, click << on the toolbar. The button is on the far right. The selected devices are then listed under the **Target list** tab. (You must use the **Target** button if you select devices from more than one group of unmanaged devices; if you only select devices from one group, however, you do not need to target the devices.)
3. Click the **Manage** tab. If you targeted the devices, select **Move targeted devices**. If you did not use the **Target** button, select **Move selected devices**.
4. Click **Move** to add the devices to the **My devices** list and places the device's information in the database.

Once the information is in the database, you can deploy the device configuration, run queries and reports on it, and perform many other management tasks.

When you move a chassis management module (CMM) to the **My devices** list, it is displayed in the **All devices** list and also as a group in the **Public groups** list. The group details show the CMM and a list of available bays in the chassis with the names of blade servers in the bays. The blade servers are also detected and managed as individual servers.

## Discovering Intel® AMT devices

Server Manager includes the option to discover devices that are configured with Intel® AMT. Devices are identified as AMT devices only if they have been correctly provisioned by the manufacturer (see [Appendix G: Intel AMT support](#)).

### To discover Intel AMT devices

1. In the left navigation pane, click **Device discovery**.
2. Click **New** to create a new configuration, and type a name for the configuration. Or click an existing configuration and click **Edit** to modify it.
3. Check **Discover Intel AMT devices**.
4. Enter starting and ending IP addresses to scan a range of addresses, and enter a subnet mask.
5. Click **Add**, then click **OK**.
6. Select the configuration and click **Schedule**. Set scheduling options, or click **Start now**, then click **Save**.
7. To view the progress of the scan, click the **Discovery tasks** tab.

AMT-configured devices are displayed in a folder labeled **Intel AMT**. From this folder you can select the device and move it to the list of managed devices.

To add the device to the inventory database in order to manage it, you must first configure the username/password for the AMT device (using the Configure Services utility), which allows Server Manager to authenticate to the AMT. This is done once for all AMT devices. This password configuration is added to the core database, which stores the information so Server Manager can authenticate to AMT devices.

If you have AMT devices with different credentials, you will need to change the credentials (using the Configure Services utility) for each device or group of devices before managing them.

#### To configure the Intel AMT password

1. Click **Start | All Programs | LANDesk | LANDesk Configure Services**.
2. Click the **Intel AMT password** tab.
3. Type the current user name and password. These must match the user name and password as configured in the Intel AMT Configuration Screen (which is accessed in the computer BIOS settings).
4. To change the user name and password, complete the **New Intel AMT password** section.
5. Click **OK**. This change will be made when the client configuration is run.

#### To move a discovered AMT device to the list of managed devices

1. Click the device name in the list of unmanaged devices.
2. Click the **Target** button on the toolbar. Click the **Manage** button on the lower pane, select **Move targeted devices**, then click **Move**.

or

Click the **Manage** button on the lower pane, select **Move selected devices**, then click **Move**.

The device is removed from the list of unmanaged devices and appears in the **All devices** list.



# Device agent installation and configuration

---

## Agent installation and configuration overview

Before you can manage devices with the console, you need to install management agents on them. You can choose to install the default agent configuration (which installs all LANDesk agents) or customize your own agent configuration to install on your devices. (The agent configuration must include the monitoring agent to receive health alerts.)

To install management agents:

- [Deploying agents](#). Target devices in the **My devices** list, then schedule an agent configuration task to remotely install agents on the devices.
- [Installing agents with an installation package](#). Create a self-extracting device installation package. Run this package locally on the device to install the agents. This must be done while logged in with administrative privileges.
- [Pulling the agent](#). Map to the core's Idlogon share (//myserver/Idlogon) and run SERVERCONFIG.EXE.

---

**Note:** You can make a device configuration the default configuration by selecting the configuration in the **Agent configuration** page and clicking **Set as default**. An IPMI BMC-only configuration cannot be a default configuration. Default configurations cannot be deleted.

---

For Windows XP Professional SP2 or 2003 SP1 systems, the settings below require manual configuration of the firewall in order for full product functionality:

### **Managed Servers:**

File and Printer Sharing - TCP 139, 445; UDP 137,138 (Push won't work without this)

Software distribution - TCP 9594, 9595 (Push won't work without this)

Advanced - ICMP - "Allow incoming echo request" (Cannot be discovered if this is not enabled.)

### **Core Server:**

Inventory – 5007

To do so, click **Start | Control Panel | Security**.

## Updating existing agents

You can push agent configurations to your devices, even if the Standard LANDesk or Remote Control agents are not yet present.

Once you've installed an agent package, installing removes the previous installation and installs the new one. You can uninstall an agent by creating a new agent package that doesn't include the agent you want removed.



## Uninstalling agents

If you need to uninstall agents from servers, follow this procedure.

### To uninstall agents from a server

1. Log in at the server with administrative rights.
2. Map a drive to the core server's LDMAIN share.
3. Open a command prompt, change to the LDMAIN share's drive letter, and enter the following:

```
uninstallwinclient.exe
```

The uninstall will run silently, removing all agents.

You can also select **Start > Run > \\core name\ldmain\uninstallwinclient.exe**.

---

**Note:** By default, Uninstallwinclient.exe reboots the device after uninstalling the agents. To avoid the reboot, you can add the /noreboot switch to the command line.

---

### To uninstall agents from a Linux server

1. Copy the linuxuninstall.tar.gz file to (a temporary directory on) the Linux box. This can be found in the LDMAIN share.

(The Linux box will likely not have Samba installed/configured, so they won't be able to copy it directly; usually they will either have to pscp it from the core, or copy it to removable media.)

2. From a shell prompt (on the Linux machine), unpack this file using tar and the x, z, and f options.

```
tar xzf linuxuninstall.tar.gz
```

3. After the file is unpacked, from a shell prompt run the linuxuninstall script from the current directory:

```
./linuxuninstall.sh
```

## Configuring agents

Before you can manage devices with the console, you need to install management agents on them. Whether you use one of the default agent configurations or create an agent configuration in the console, you can install it on Windows or Linux devices in one of three ways:

- Create a self-extracting installation package. Run this package locally on the device to install the agents. This must be done while logged in with administrative privileges. For more information, see ["Installing agents with an installation package."](#)
- Target devices in the **My devices** list, then schedule an agent configuration task to remotely install agents on the devices.
- From a Windows device, map to the core's ldlogon share (\\myserver\ldlogon) and run SERVERCONFIG.EXE.

### To create an agent configuration

1. In the left navigation pane, click **Agent configuration**.
2. Click **New**.
3. Type a name for the new configuration in the **Configuration name** box.

Type a name that describes the configuration you're working on. This can be an existing configuration name or a new one. This name appears on the settings file icon in the **Server setup** window.

4. Select the type of configuration you want, then click **OK**.
5. Select the configuration you just created, and click **Edit**.

In the tabs, some options are dimmed because they are not configurable for the configuration you chose. For example, remote control is not configurable for a Linux configuration because SSH is used.

6. In the **Agent** tab, select the agents you want to deploy.
  - **All:** Installs all agents on the selected device.
  - **Standard LANDesk agent:** Formerly the common base agent (CBA), in Management Suite, it forms the basis of communication between devices and the core server. This is a required agent. Most of this agent's processes are on-demand.
  - **Remote control:** Installs the remote control agent on the selected device. This lets you use a special application-level version of remote control for extra reliability. By running remote control at the application level instead of the driver level, the server won't be as vulnerable to remote control problems. This agent can be run on-demand if the on-demand option is selected in the **Agent configuration** dialog.
  - **Remote control mirror driver:** Installs the remote control mirror driver, which reduces the amount of time required to see the targeted machine's desktop. This is not an on-demand agent.
  - **Vulnerability scanner:** Installs the patch manager vulnerability scanner. With this agent installed, you can configure how the scanner runs. This is not an on-demand agent.
  - **Software distribution:** Installs the SWD agent on the selected device. This allows for automating the process of installing software applications or distributing files to devices. Use this to install applications simultaneously to multiple devices or to update files or drivers on multiple devices. This is an on-demand agent.
  - **Monitoring:** Installs the monitoring agent on the selected server. The monitoring agent allows for many types of monitoring, including direct ASIC monitoring, In band IPMI, Out of band IPMI, and CIM. This is not an on-demand agent.
7. In the **Configuration** system type boxes, select the type. If this is dimmed, it is because you have already selected the type.
8. Select a **Reboot** option.

Rebooting manually means that devices will not reboot after installation. A device reboot is not required after agent configuration. You must manually reboot the device.

Rebooting if necessary causes a reboot for agent updates when updated files are locked.

9. In the **Inventory** tab, set the Inventory Scanner configuration settings. These are explained below.
  - **Automatic update:** Remote devices read the software list from the core server during software scans. If this option is set, each device must have a drive mapped to the LDLOGON directory on the core server so they can access the software list. Changes to the software list are immediately available to devices.
  - **Manual update:** The software list used to exclude titles during software scans is loaded down to each remote device. Each time the software list is changed from the console, you must manually resend it to remote devices.
  - **Inventory scanning settings:** The drop-down list beside this option allows you to select from **Frequency**, **Between the hours of**, and **Always run on startup**. If you have users run the scanner manually, they can launch it from **Start | Programs | LANDesk Management | Inventory Scan**.  
 If you select the inventory scanner **Between the hours of** option, you can specify an hour range that the scanner can run between. If a device logs in during the time range you specify, the inventory scan runs automatically. If the device is already logged in, once the starting hour arrives the inventory scan starts automatically. This option is useful if you want to stagger inventory scans on devices so they don't send scans all at once.
  - **Always run at startup:** Runs the Inventory scanner on startup of the device.

10. In the **Remote control** tab, select the type of agent to install.

**Service:** The agent runs as a service, and runs in the background. It uses NT-based security. If you want to add users or groups to use NT-based remote control, you must add them to the Remote Control Operators group.

**On-demand:** The agent only runs when needed. It uses certificate-based security.

11. In the **Monitoring** tab, select any monitoring and/or alerting rulesets you want included with the configuration. These rulesets are stored in the Idlogon/alertrules folder. New rulesets can be created in Monitoring or Alerting.
12. Click **Save changes** to save the information to the database. Click **Save as file** to save the configuration as a distributable package.

---

**Note:** You can make an agent configuration the default configuration by selecting the configuration in the **Agent configurations** page and clicking **Set as default**. An IPMI BMC-only configuration cannot be a default configuration. Default configurations cannot be deleted.

---

**To schedule an agent task**

1. In the left navigation pane, click **Agent configuration**.
2. Create an agent configuration.
3. Click the agent configuration and click **Schedule task**.
4. In the bottom pane, click the task you just created and click **Edit**.
5. Review the list of [targeted devices](#) and the task schedule.
6. Click **Save**.

When you click **Schedule task**, a task is created (it has no targeted devices, and it is unscheduled). If you cancel this Scheduled task procedure, please be aware that it has still been created and appears in the Task list.

## Deploying agents to managed devices

Once you have discovered devices, you can deploy agents to them. You can only deploy agents to supported Windows and Linux OS devices. You must have Administrator rights to deploy agents to Windows devices, and the root privilege to configure Linux devices.

You can deploy agents to unmanaged devices in one of these ways:

- Push-based deployments using a discovery job and a domain administrative account you've configured for the scheduler service, which processes discovery jobs. The domain administrative account gives the scheduler services the rights it needs to install the server agents. This works for Windows NT family servers.
- Push-based deployments using the Standard LANDesk agent (formerly known as CBA or common base agent in Management Suite). If the servers have the Standard LANDesk agent, which is used by many LANDesk Software products, you can deploy to them without requiring a domain administrative account.

When deploying to discovered devices, use the **Unmanaged** tree's **Filter by** option. You can filter on IP address to isolate devices.

---

If you try to use an LDAP query or an LDAP target for the initial deployment of an agent, the attempt will fail. This is because the LDAP location information is not in the database.

---

For Windows XP Professional SP2 or 2003 SP1 systems, the settings below require manual configuration of the firewall in order for full product functionality:

**Managed Servers:**

File and Printer Sharing - TCP 139, 445; UDP 137,138 (Push won't work without this)

Software distribution - TCP 9594, 9595 (Push won't work without this)

Advanced - ICMP - "Allow incoming echo request" (Cannot be discovered if this is not enabled.)

**Core Server:**

Inventory – 5007

To do so, click **Start | Control Panel | Security**.

## Configuring device authentication credentials

Unmanaged devices with the Standard LANDesk agent on them don't require authentication credentials for agent deployment. To install agents on Windows OS servers that don't have the Standard LANDesk agent, you must specify the credentials that the scheduler service on the console device will use to get the required rights.

To install device agents on unmanaged devices, the scheduler service needs to be able to connect to devices with an administrative account. The default account the scheduler service uses is LocalSystem. The LocalSystem credentials generally work for devices that aren't in a domain.

If devices are in a domain, you must specify a domain administrator account. If you're configuring unmanaged devices in multiple domains, you must configure them one domain at a time, since the scheduler service authenticates with one set of credentials, and each domain will require a different domain administrator account.

The core server includes a utility, SVCCFG.EXE, that you can use to customize inventory options. You can run SVCCFG.EXE from the core server's Start\Program Files\LANDesk\Configure Services. You must run SVCCFG.EXE at the core server.

### To configure the scheduler service login credentials

1. Launch SVCCFG.EXE on the console server.
2. Click the **Scheduler** tab.
3. Click the **Change Login** button.
4. Enter the credentials you want the service to use on clients, typically a domain administrator account.

## Installing agents

Once you've created an agent configuration in the console, you need to install it on devices.

Client agent packages are a single self-extracting executable file. By default they're stored in the "C:\Program Files\LANDesk\ManagementSuite\ldlogon" folder on the core server. Running the executable installs the client agents silently, without requiring any user interaction.

### Installing agents

You can update the agents by creating a new client configuration and distributing it from the console, or install agents directly to unmanaged devices.

Once you've installed a client agent package, installing other client agent packages removes all agents and installs the agents specifically selected. You can uninstall an agent by creating a new client agent package that doesn't include the agent you want removed.

## Uninstalling agents

If you need to uninstall agents from devices, please see [Agent installation and configuration overview](#).

## Installing agents with an installation package

One of the ways you can install agents is with a self-extracting device agent package. This allows you to copy the file to a CD or USB drive to install agents manually. You can create these packages by clicking **Save as file** in the bottom of the **Configuration** dialog.

1. Click **Agent configuration**, then double-click a configuration name.
2. In the **Agent configuration** dialog, click **Save as file**, then click **Close**.

Clicking **Save as file** creates a self-extracting executable package with the filename matching the configuration name you specified. It might be a few minutes before the package is available in the "\\Program Files\\LANDesk\\ManagementSuite\\ldlogon\\ConfigPackages" folder on the core server.

Running the executable installs the agents, without requiring any user interaction. You must log in with administrative privileges.

---

If your users can't log in with administrative privileges to install the package, you can deploy the packages via e-mail, Web download, login scripts, or from a share.

---

## Pulling the agents

This section contains details on deploying agents from the command line. You can control what components are installed on devices by using SERVERCONFIG.EXE command-line parameters. You can launch SERVERCONFIG.EXE in standalone mode. It's located in the *http://coreserver/LDLogon* share, which is readable from any Windows server.

SERVERCONFIG.EXE uses SERVERCONFIG.INI for configuring devices.

## Understanding SERVERCONFIG.EXE

SERVERCONFIG.EXE configures Windows NT family servers for management in four steps:

1. SERVERCONFIG determines whether the computer has been previously configured. If it has, SERVERCONFIG removes all components and reinstalls selected components.
2. If SERVERCONFIG loads the appropriate initialization file (SERVERCONFIG.INI) and executes the instructions contained in it.

The following command-line parameters are available for SERVERCONFIG.EXE:

Parameter	Description
/I	<p>Components to include (quotation marks included):</p> <p>"Common Base Agent"</p> <p>"Inventory Scanner"</p> <p>"Alerting"</p> <p>"Remote Control"</p> <p>"Mirror Driver"</p> <p>"Vulnerability Scanner"</p> <p>"Software Distribution"</p> <p>"Server Monitor"</p> <p>You can combine these on the same command line. For example:</p> <pre>SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability Scanner"</pre>
/IP	Configure using IP
/L or /Log=	Path to the CFG_YES and CFG_NO log files that log which servers were and were not configured
/LOGON	Execute [LOGON] prefixed commands
/N or /NOUI	Do not display the user interface
/NOREBOOT	Don't reboot server when done
/REBOOT	Force reboot after running
/TCPIP	Configure using IP
/X=	<p>Components to exclude. For example:</p> <pre>SERVERCONFIG.EXE /X=SD</pre>
/CONFIG= /[CONFIG]=	<p>Specifies a server configuration file to use in place of the default SERVERCONFIG.INI files.</p> <p>For example, if you've created configuration files called NTTEST.INI, then use this syntax:</p> <pre>SERVERCONFIG.EXE /CONFIG=TEST.INI</pre> <p>The custom .INI files should be in the same directory as SERVERCONFIG.EXE and note that the /config parameter uses the filename without the NT prefix.</p>
/? or /H	Display help menu

## Creating an agent configuration

Use **Agent configuration** to create and update server agent configurations (such as what agents are installed on managed). You can create different configurations for a group's specific needs. For example, you could create a configuration for Web servers and another one for application servers.

To push a configuration to a server, you need to:

- **Create the agent configuration:** Set up specific configurations for your servers.
- **Schedule the agent configuration:** Push the configuration to servers or, from the server, run SERVERCONFIG.EXE from the core server's LDLogon share.

### To create an agent configuration

1. In the console, click **Agent configuration**.
2. Click the **New** toolbar button.
3. Enter a **Configuration name** and select the operating system, then click **OK**.
4. Click the new configuration name, then click **Edit**.
5. Select the agents you want to deploy.
6. Use the tabs on the top of the dialog to navigate to options relating to the components you selected. Customize the options you selected as necessary.
7. Click **Save changes**, then close the dialog.
8. If you want the configuration to be the default, click **Set as default**.

## Pulling a Linux agent configuration

To pull Linux agents, please see [Installing Linux server agents](#), "To pull a Linux configuration."

1. Copy the following files from the LDLOGON share:

\*.0 (the "dot zero" files are the certificates for the Common LANDesk Agent - there should be one .0 file)

<configuration name>.sh (substitute your configuration name here)

unix\linux\baseclient.tar.gz

unix\linux\monitoring.tar.gz

unix\linux\vulscan.tar.gz

2. Copy the files on the Linux device you are to pull from to a temporary directory, such as "/tmp/ldcfg".
3. If the machine is an IPMI/BMC machine (with monitoring included in the installation), type the following on a command line:

```
export BMCPW="(bmc password)"
```



4. Running as root, execute the shell script for the configuration. For example, if you named the script "basic-linux," use the full path used in step 2:

```
/tmp/ldcfg/basic-linux.sh
```

---

**Note:** Please be aware that if you push or pull an agent out to a Linux machine, then run the `linuxuninstall.sh -f ALL`, to clean it (which deletes the GUID as it should) and then push or pull again, this process creates duplicate database entries for the same machine with the same name and IP.

---

## Creating standalone agent configuration packages

Normally the client configuration utility, `SERVERCONFIG.EXE`, configures clients. If you want, you can have the **Agent configuration** window create a self-extracting single-file executable that installs an agent configuration on the server it's run on. This is helpful if you want to install agents from a CD or portable USB drive.

## Pushing an agent configuration to devices

### To push an agent configuration to a preexisting agent

1. In the console, select the devices you want to deploy the agent to, then click **Target**.
2. In the left navigation pane, click **Agent configuration**.
3. Right-click the agent configuration you want to push, then click **Schedule task**.
4. Click **Target devices** in the **Schedule task properties** dialog box, then click **Add target list**.
5. Click **Save**.
6. Specify the time to deploy the agent, then click **Save**.

## Installing Linux server agents

You can remotely deploy and install Linux agents and RPMs on Linux servers. Your Linux server must be configured correctly for this to work. To install an agent on a Linux server, you must have root privileges.

The default Red Hat Enterprise 3 Linux AS and ES install includes the RPMs that the Linux standard LANDesk agent requires. If you select the monitoring agent in **Agent configuration**, you need two additional RPMs, `perl-CGI` and `sysstat`. For the complete list of RPMs that the product requires, see the *Server Manager Deployment Guide*.

For an initial Linux agent configuration, the core server uses an SSH connection to target Linux servers. You must have a working SSH connection with username/password authentication. This product doesn't support public key/private key authentication. Any firewalls between the core and Linux servers need to allow the SSH port. Consider testing your SSH connection from the core server with a 3rd-party SSH application.

The Linux agent installation package consists of a shell script, agent tarball(s), .INI agent configuration, and agent authentication certificates. These files are stored in the core server's LDLogon share. The shell script extracts files from the tarball(s), installs the RPMs, and configures the server to load the agents and run the inventory scanner periodically at the interval you specified in the agent configuration. Files are placed under /usr/LANDesk.

You must also configure the scheduler service on the core to use the SSH authentication credentials (username/password) on your Linux server. The scheduler service uses these credentials to install the agents on your servers. Use the [Configure services utility](#) to enter the SSH credentials you want the scheduler service to use as alternate credentials. You should be prompted to restart the scheduler service. If you aren't, click **Stop** and then **Start** on the **Scheduler** tab to restart the service. This activates your changes.

## Deploying the Linux agents

After you've configured your Linux servers and added Linux credentials to the core server, you must add servers to the **My devices** list so you can deploy the Linux agents. Before you can deploy to a server, you must add it to the **My devices** list. Do this by discovering your Linux server with **Discover devices**.

### To discover your Linux servers

1. In **Device discovery**, create a discovery job for each Linux server. Use a standard network scan and enter the Linux server's IP address for the starting and ending IP ranges. If you have many Linux servers, enter a range of IP addresses. Click **OK** once you've added your discovery IP ranges.
2. Schedule the discovery task that you just created by clicking it and clicking **Schedule**. When the task finishes, verify **Device discovery** found the Linux servers you want to manage.
3. In **Device discovery**, select the servers you want to manage and click the **Manage** tab in the lower half of the window. Click **Move selected devices** and click **Move**. This adds the servers to the **My devices** list, so you can target them for deployment.

### To create a Linux agent configuration

1. In **Agent configuration**, click **New**.
2. Enter a configuration name, click **HP-UX** or **Linux Server Edition**,, and click **OK**.
3. Select the configuration you just created and click **Edit**.
4. Select the agents you want.
5. In the **Inventory** tab, select the options and the scanner frequency interval that you want. The installation script will add a cron job that runs the scanner at the interval you select.
6. Click **Save changes**.

To deploy your agent configuration, select it in **Configure agents** and click **Schedule task**. Configure the task and monitor the task progress in **Configuration tasks**.

**To pull a Linux agent configuration**

1. Copy all the files from the the LDLOGON\unix\linux directory, and place the files on the Linux box you are to pull from in a temporary directory, such as "/tmp/ldcfg".
2. If the machine is an IPMI/BMC machine (with Monitoring included in the installation), type the following on a command line:

```
export BMCPW="(bmc password)"
```

3. Running as root, execute the shell script for the configuration. For example, if you named the script "basic-linux," use the full path used in step 2:

```
/tmp/ldcfg/basic-linux.sh
```

---

**Note:** Please be aware that if you push or pull an agent out to a Linux machine, then run the linuxuninstall.sh -f ALL, to clean it (which deletes the GUID as it should) and then push or pull again, this process creates duplicate database entries for the same machine with the same name and IP.

---

**Inventory scanner command-line parameters**

The inventory scanner, ldiscan, has several command-line parameters that specify how it should run. See "ldiscan -h" or "man ldiscan" for a detailed description of each. Each option can be preceded by either '-' or '/'.

Parameter	Description
-d=Dir	Starts the software scan in the Dir directory instead of the root. By default, the scan starts in the root directory.
-f	Forces a software scan. If you don't specify -f, the scanner does software scans on the day interval (every day by default) specified in the console under <b>Configure   Services   Inventory   Scanner Settings</b> .
-f-	Disables the software scan.
-i=ConfName	Specifies the configuration filename. Default is /etc/ldappl.conf.
-ntt=address:port	Host name or IP address of core server. Port is optional.
-o=File	Writes inventory information to the specified output file.
-s=Server	Specifies the core server. This command is optional, and only exists for backward compatibility.
-stdout	Writes inventory information to the standard output.
-v	Enables verbose status messages during the scan.
-h or -?	Displays the help screen.

## Examples

To output data to a text file, type:

```
ldiscan -o=data.out -v
```

To send data to the core server, type:

```
ldiscan -ntt=ServerIPName -v
```

## Linux inventory scanner files

File	Description
ldiscan	The executable that is run with command-line parameters to indicate the action to take. All users that will run the scanner need sufficient rights to execute the file.  There is a different version of this file for each platform supported above.
/etc/ldiscan.conf	This file always resides in /etc and contains the following information: <ul style="list-style-type: none"> <li>• Inventory assigned unique ID</li> <li>• Last hardware scan</li> <li>• Last software scan</li> </ul> All users who run the scanner need read and write attributes for this file. The unique ID in /etc/ldiscan.conf is a unique number assigned to a computer the first time the inventory scanner runs. This number is used to identify the computer. If it ever changes, the core server will treat it as a different computer, which could result in a duplicate entry in the database.  <b>Warning:</b> Do not change the unique ID number or remove the ldiscan.conf file after it has been created.
/etc/ldappl.conf	This file is where you customize the list of executables that the inventory scanner will report when running a software scan. The file includes some examples, and you'll need to add entries for software packages that you use. The search criteria are based on filename and file size. Though this file will typically reside in /etc, the scanner can use an alternative file by using the -i= command-line parameter.
ldiscan.8	Man page for ldiscan.

## Console integration

Once a Linux computer is scanned into the core database, you can:

- Query on any of the attributes returned by the Linux inventory scanner to the core database.
- Use the reporting features to generate reports that include information that the Linux scanner gathers. For example, Linux will appear as an OS type in the Operating Systems Summary Report.

- View inventory information for Linux computers.

---

**Queries on "System Uptime" sort alphabetically, returning unexpected results**

If you want to do a query to find out how many computers have been running longer than a certain number of days (for example, 10 days), query on "System Start" rather than "System Uptime." Queries on System Uptime may return unexpected results, because the system uptime is simply a string formatted as "x days, y hours, z minutes, and j seconds." Sorting is done alphabetically and not on time intervals.

**Path to config files referenced in `ldappl.conf` doesn't appear in the console**  
ConfFile entries in `ldappl.conf` file need to include a path.

---

# Device monitoring

---

## About monitoring

Server Manager provides several methods of monitoring a device's health status. Server Manager supports many types of monitoring, including direct ASIC monitoring, in-band IPMI, out-of-band IPMI, CIM, and so forth. Monitoring lets you keep track of many pieces of data on your devices, such as:

- Usage levels
- OS events
- Processes and services
- Historical performance
- Hardware sensors (fans, voltages, temperatures, etc.)

This chapter includes information about the different features that monitor your managed devices:

- [Installing a monitoring agent](#) on devices and creating monitoring configurations that can be deployed to devices
- [Setting performance counters](#) on devices and monitoring the performance data
- [Monitoring configuration changes](#) with alerts when changes occur
- Pinging devices regularly to [monitor their connectivity](#), using the **Device monitor** feature

Alerting is a related feature that uses the monitoring agent to initiate alerting actions such as sending e-mail or pager messages, rebooting or shutting down a device, or adding information to the alert log. You can generate alerts from any of the device events that can be monitored. See [Using alerts](#) for more information.

### Notes

- Communications to the monitoring agent are via HTTP over TCP/IP in the form of GET, POST, or XML requests. Responses to requests are in XML or HTML table documents.
- To run and store a query on the health status of devices (Computer.Health.State), you should be aware that the state in the database is represented by a number. The numbers correspond to the following states: 4=Critical, 3=Warning, 2=Normal, 1=Informational, null or 0=unknown.
- Hardware monitoring is dependent on the capabilities of the hardware installed on a device, as well as on the correct configuration of the hardware. For example, if a hard drive with S.M.A.R.T. monitoring capabilities is installed on a device but S.M.A.R.T. detection is not enabled in the device's BIOS settings, or if the device's BIOS does not support S.M.A.R.T. drives, monitoring data will not be available.

## Deploying the monitoring agent to devices

Server Manager provides an immediate summary of a device's health when the monitoring agent is installed on the device. The monitoring agent is one of six agents that can be installed on managed devices. It checks the device's hardware and configuration on a regular, periodic basis and reflects any changes in the device's health status. This is shown by the status icon in the **My devices** list, and details are displayed in log entries (shown in the **System information** summary for the device) and in graphs (shown in the **Monitoring** summary page for the device).

For example, a monitored device with a disk drive that is filling up can display a warning status icon when the disk is 90% full, changing to a critical status icon when the disk is 95% full. You may also receive alerts for the same disk drive status if the device has an alert configuration that includes rules for a drive space alert.

You can deploy the default monitoring configuration to devices. Or, if you prefer, you can create a custom configuration that includes only the health items you're concerned with.

## Creating a monitoring configuration

You can choose what is monitored on a device by creating a monitoring configuration, which is a ruleset that defines what the monitoring agent checks on the device. You can deploy a configuration to one device or a targeted group of devices. For example, you may define one configuration for servers dedicated to storage and use a different configuration for Web servers.

The default monitoring configuration includes 17 items. When you create a configuration you can turn any of these items on or off, specify how frequently to check them, and, for some items, set performance thresholds. You can also select services running on the devices that you want to monitor.

### To create a monitoring configuration

1. In the left navigation pane, click **Monitoring**.
2. Click **New**, type a name and description for the configuration, and click **OK**.
3. Select the configuration.
4. In the list of items, click an item you want to change and click **Edit**.
5. To turn off monitoring of the item, clear the checkbox and click **Update**.
6. To change the frequency at which the item is monitored, select **Seconds** or **Minutes** and specify a number in the text box.
7. If applicable, set the threshold percentages for warning and critical status.
8. For **Services** monitoring, select the OS from the drop-down list. Select one or more services to monitor (use CTRL + click to select more than one) and click **>>** to add the services to the list on the right.
9. For each item that you modify, click **Update** to apply your changes to the configuration.

### To deploy a monitoring configuration

1. In the left navigation pane, click **My devices**, then click the **All devices** group.

2. Select the devices to which you want to deploy the alert configuration, then click **Target** to place the devices in the **Targeted devices** list.
3. In the left navigation pane, click **Monitoring**, then click the **Deploy configuration** tab.
4. In the **Monitoring configurations** box, select the configuration you want to deploy.
5. Click the link to view the **Targeted devices** list. To remove a device from this list, right-click it, then click **Remove**. (To add devices, you must add them to the targeted list as described in step 2.)
6. Click **Deploy** to deploy the selected configuration to the targeted devices.

As part of the deployment process, an XML page is created that lists the deployed configurations and devices the configurations were deployed to. This report is saved on the core server in the LDLOGON directory, and is named with a sequential number assigned by the database. If you want to view this XML page separately from deploying a configuration, click the **Generate XML** button and then click the link to view the XML file.

## Turning off the ModemView service

The ModemView service is the service/driver that monitors modem calls (both incoming and outgoing) and generates an alert if it sees one. This service uses about 10 Mb of memory because it uses MFC. You may not want it to be running, especially if you don't have a modem on the device.

### To turn the ModemView service off

1. On the device (either directly or via remote control) click **Start > Control Panel > Administrative Tools > Services**.
2. Double-click **LANDesk Message Handler Service**.
3. Under **Startup Type**, select **Manual**, and click **OK**.

You can also click **Stop** under **Service Status**.

## Setting performance counters

Server Manager lets you select performance items (counters) that you want to monitor on a managed device. You can monitor many different kinds of items including hardware components, such as drives, processors, and memory, or OS components, such as processes, or application components, such as bytes per second transferred by the system's Web server. When you select a performance counter you also specify the frequency for polling the item, as well as specify the performance thresholds and number of violations that are allowed before an alert is generated.

When a performance counter has been selected, you can then monitor performance on the Monitoring page by viewing a graph with real time or historical data. See [Monitoring performance](#) for more details.



**To select a performance counter to monitor**

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.

The summary opens in another browser window.

3. In the left navigation pane, click **Monitoring**.
4. Click the **Performance counter settings** tab.
5. From the **Objects** column, select the object you want to monitor.
6. From the **Instances** column, select the instance of the object you want to monitor, if applicable.
7. From the **Counters** column, select the specific counter you want to monitor.
8. Specify the polling frequency (**Check every *n* seconds**) and the number of days to keep the counter history.
9. In the **Alert after counter is out of range** drop-down list, specify the number of times the counter will be allowed to cross the thresholds before an alert is generated.
10. Specify upper and/or lower thresholds.
11. Click **Apply**.

**Notes**

- Performance log files can quickly grow in size; polling a single counter at a two second interval adds 2.5 MB of information to the performance log daily.
- Changing the **Alert after counter is out of range** number lets you choose to focus on an issue when it is a persistent problem or when it is an isolated event. For example, if you are monitoring the bytes sent from a Web server, Server Manager can alert you when the bytes/sec consistently runs high. Or, you can specify a low number such as 1 or 2 to get alerted whenever your anonymous FTP connections exceed a certain number of users.

## Monitoring performance

The Monitoring page lets you monitor the performance of various system objects. You can monitor specific hardware components, such as drives, processors, and memory, or you can monitor OS components, such as processes or bytes per second transferred by the system's Web server. The Monitoring page includes a graph that displays real-time or historical data for counters.

In order to monitor a performance counter you must first select the counter, which adds it to the list of monitored counters. When you do this you also specify the frequency for polling the item and set performance thresholds and the number of violations that are allowed before an alert is generated. See [Performance counters](#) for details on selecting counters.

**To view a performance graph for a monitored counter**

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.

The local console opens in another browser window.


3. In the left navigation pane, click **Monitoring**.
4. Click the **Active performance counters** tab, if necessary.
5. From the **Counters** drop-down list, select the counter you for which want to see a performance graph.
6. Select **View real-time data** to display a graph of real-time performance.

or

Select **View historical data** to display a graph showing performance over the period you specified (Keep history) when selecting the counter.

On the performance graph, the horizontal axis represents time that has passed. The vertical axis represents the units you are measuring, such as bytes per second (when monitoring file transfers, for example), percentage (when monitoring percentage of the CPU that is in use), or bytes available (when monitoring hard drive space). The line height is not a fixed unit. The height of the line changes relative to the extremes in the data; for one counter the vertical axis might represent 1 to 100 and for another it might represent 1 to 500,000. When the data varies across a wide extreme, minimal changes can appear as a flat line.

### Notes

- Selecting another counter refreshes the graph and resets the units of measurement.
- Click  to clear and restart the graph.
- Click **Reload counters** to refresh the list with any new objects, instances, or counters.
- If you receive an alert generated by a counter in the list, select the counter and click **Acknowledge** to clear the alert.

### To stop monitoring a performance counter

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.

The local console opens in another browser window.

3. In the left navigation pane, click **Monitoring**.
4. Click the **Active performance counters** tab, if necessary.
5. Under **Monitored performance counters**, select the counter and click **Delete**.

## Monitoring configuration changes

This product can [generate alerts](#) if a device's hardware or software configuration changes and the monitoring agent is installed on the device. These changes may affect a device's performance and stability or cause problems with a standard

installation. By monitoring vital pieces of the device, this product can reduce total cost of ownership (TCO).

The device configuration changes that will generate alerts are:

- **Application installed or uninstalled:** You can see which users installed or removed applications. This may be helpful in tracking licenses or employee productivity. Applications registered in the Windows Add/Remove Programs area of the Control Panel are monitored. Other applications are ignored. The application name that is used in the Windows Add/Remove Programs is the application name that appears in the notification log or alert pop-ups window.
- **Memory added or removed:** This product detects and monitors the quantity and type of memory installed. If the configuration changes, an alert is generated.
- **Hard drives added or removed:** This product detects and monitors the type and size of the drives installed on devices. If the configuration changes, an alert is generated.
- **Processor (or processors) added, removed, or modified:** This product detects and monitors the number, type, and speed of the processor(s). If the configuration changes, an alert is generated.
- **Network card added or removed:** This product detects and monitors the number and type of network interface cards on devices, and generates alerts when the configuration changes.

To view a record of alerts for configuration changes, review the alert log on the device's console. See [Viewing the alert log](#) for details.

## Monitoring for connectivity

In most cases, devices can alert you when critical situations arise, such as when the hard disk is filling up or a fan has stopped. However, in some situations, the device can go offline before it can send an alert. For example, a switch or router may disrupt network traffic, or the device may experience power failure.

In these situations, this product can check on devices periodically to determine whether they are available on the network. If the device does not respond to the ping, its health status is changed to critical in the dashboard (or the next time you refresh the **My devices** list).

You must set up the device monitor to ping targeted devices or all devices in the **All devices** group.

### To set up the device monitor

1. In the **My devices** list, select the devices you wish to monitor. You can select them from **All devices** or from a public or private group.
2. Click **Target**.
3. In the bottom pane, click **Actions**, and click **Device monitor**.
4. To view a list of devices currently being monitored, click **Show monitored devices**.
5. Type numbers for the minutes between ping sweeps and number of times the product will attempt to communicate with a device.
6. Select whether to perform the action on devices in the [Targeted devices list](#) or on all devices in the **All devices** group.
7. Click **Apply**.

Only the last group of targeted devices are monitored. For example, if you target device A and device B and apply device monitoring to them, only device A and device B will be pinged by the core server. If you then target device C and device D and apply device monitoring to those devices, only device C and device D will be monitored; devices A and B will no longer be monitored.



# Alert configuration

---

## Using alerts

When a problem or other event occurs on a device (for example, the device is running low on disk space), Server Manager can send an alert. You can customize these alerts by choosing the severity level or threshold that will trigger the alert. Alerts are sent to the console and can be configured to perform specific actions. Use this chapter to understand how alerts work.

- [How do I see alerts?](#)
- [What kinds of device problems can generate alerts?](#)
- [Configuring severity levels for events](#)
- [Example: Configuring an alert for a disk space problem](#)

## How do I see alerts?

This product can notify you of problems or other computer events by:

- Adding information to the log
- E-mailing a notice or sending a message to a pager
- Running a program on the core or an individual device
- Sending an SNMP trap to an SNMP management console on the network
- Rebooting or shutting down a device

Please be aware that certain alerts assigned to groups of machines can simultaneously generate a large number of responses. For example, you can set the alert “Computer configuration change” and associate it with an e-mail action. If a software distribution patch is applied to those machines with this alert setting, it would generate a number of e-mails from the core server equal to the number of machines to which the patch was applied, potentially “flooding” your e-mail server. In this case, an option might be to handle this alert by simply writing it to the core log rather than send e-mail.

## What kinds of device problems can generate alerts?

This product has an extensive list of events that can generate alerts. Some are problems that need immediate attention; others are configuration changes that may or may not be a problem but that provide useful information to a system administrator. (See [Monitoring configuration changes](#) for related information.) Alerts can only be generated when devices are equipped with the appropriate hardware. For example, alerts generated from sensor readings are only applicable to devices equipped with the correct sensors.

The types of events that you can potentially monitor include the following:

- **Hardware change:** A component such as a processor, memory, a drive, or a card has been added or removed.

- **Application added or removed:** An application has been installed or uninstalled on a device.
- **Service event:** A service has started or stopped on the device.
- **Performance:** A performance threshold has been crossed, such as for drive capacity, available memory, etc.
- **IPMI event:** An event detectable on IPMI devices has occurred, including changes to controllers, sensors, logs, etc.
- **Modem usage:** The system modem has been used, or a modem has been added or removed.
- **Physical security:** Chassis intrusion detection, power cycling, or another physical change has occurred.
- **Package installation:** A package has been installed on the target computer.
- **Remote control activity:** Remote control session activity has occurred, including starting, stopping, or failures.

Hardware monitoring that generates alerts is dependent on the capabilities of the hardware installed on a device, as well as on the correct configuration of the hardware. For example, if a hard drive with S.M.A.R.T. monitoring capabilities is installed on a device but S.M.A.R.T. detection is not enabled in the device's BIOS settings, or if the device's BIOS does not support S.M.A.R.T. drives, alerts will not be generated from S.M.A.R.T. drive monitoring.

## Configuring severity levels for events

Device problems or events can be associated with some or all of the severity levels shown below.

- **Informational:** Supports configuration changes or events that manufacturers may include with their systems. This severity level does not affect device health.
- **OK:** Indicates that the status is at an acceptable level.
- **Warning:** Provides some advance warning of a problem before it reaches a critical point.
- **Critical:** Indicates that the problem needs immediate attention.
- **Unknown:** The alert status cannot be determined or the monitoring agent has not been installed on the device.

Depending on the nature of the event or server problem, some severity levels don't apply and aren't included. For example, with the Intrusion detection event, the device's chassis is either open or closed. If it is open, this can trigger an alert action with a severity of Warning. Other events, such as Disk space and Virtual memory, include three severity levels (OK, Warning, and Critical).

You can choose the severity level or threshold that will trigger some alerts. For example, you can select different actions as a result of a Warning or Critical status for an alert. The Unknown status can't be selected as an alert trigger but simply indicates that the status cannot be determined.

## Configuring alerts

You can configure an alert ruleset to deploy to an individual device or to a group of targeted devices. Each managed device must have the LANDesk monitoring component installed before it can send alerts to the core server. (See [Configuring client agents](#) for more information.)

When the monitoring component is installed to a managed device, a default ruleset of alerts is included to provide health status feedback to the dashboard and console. This default ruleset includes alerts such as:

- Disk added or removed
- Drive space
- Memory usage
- Temperature, fans, and voltages
- Remote control activities
- Performance monitoring
- IPMI events (on applicable hardware)

In addition to the default ruleset, you can configure and deploy custom alert rulesets. You can include custom alert actions to respond a particular event. For example, if a fan stops, it can trigger an alert and send an e-mail to your hardware support group.

We recommend that you create alert action configurations before creating custom alert rulesets, because you can't select an action if it has not been configured. (See [Configuring alert actions](#) for more information.) If you plan to deploy a configuration when you create it, select the devices and target them before configuring the alert, as shown in the following example.

### Example: Configuring an alert for a disk space problem

1. In the left navigation pane, click **My devices**, then double-click the **All devices** group.
2. Select the devices for which you want to set the alert, then click **Target** to place the devices in the **Targeted devices** list.
3. Click **Alerting**, then click the **Alert configurations** tab.
4. Click **New**, type something like "Disk Space Problem" in the **Name** field, type a description in the **Description** field, and click **OK**.
5. Click the alert you just named, click **Edit configuration**, then click **New**.
6. In the **Alert type** drop-down list, select **Drive space**.
7. Check the status you wish to alert on: **OK**, **Warning**, or **Critical**. (If you want the same action for multiple statuses, select more than one. If you want a different action for each status, create a separate configuration for each status so you can trigger different actions for different status levels.)
8. In the **Action** drop-down list, select the action you want to occur if the conditions specified in steps 6 and 7 are met. If the action you want is not on the list, you can [create](#) it using the **Action configuration** page. (If you have not configured an alert action it will not be in the list.)
9. In the **Action configuration** drop-down, select the configuration you want.
10. Check **Affects device health** if you want the alert to apply to the server's health state when it is displayed in the dashboard or the **All devices** list. If



the severity level for the alert is **Informational** only, the alert will not affect device health.

11. Click **Add**.
12. Repeat steps 6-11 if you want to add additional alerts to the ruleset.
13. When finished, click **Close**.

To apply the alert configuration to selected devices you must deploy the configuration (see "[Deploying configurations](#)").

## Configuring alert actions

Use the **Action configurations** page to provide additional information for how you want the actions to behave when they are selected. When a threshold is crossed, an alert is generated. The alert can have an action associated with it, such as sending an e-mail. Each action has its own configurations, and must be set up individually.

### To create an action configuration

1. In the left navigation pane, click **Alerting**, then click the **Action configurations** tab.
2. In the **Actions** drop-down list, select the action you want to configure. Each action has its own list of unique configurations.
3. Click **New**, type a name in the **Name** field, then click **OK**.
4. Back in the **Action configurations** page, select the configuration you just named, and click **Edit configuration**.
5. If you selected **Execute program on core** or **Execute program on client**, type or paste the path to the program you want to execute on the alert, then click **Save**.

If you selected **Send e-mail/page**, type the full e-mail address of the person you want to receive the e-mail in the **To** field; type the name of the person, group, or entity responsible for the e-mail in the **From** field; type a subject in the **Subject** field; type a message in the **Body** field; select the day or time you want to have the message sent; and type the location of an SMTP server in the **SMTP server** field. Click the **Help** box to learn how to send messages to multiple recipients and how to use variables in your messages. When you have finished, click **Save**.

If you selected **Send an SNMP trap**, type the host name, select a version, type the community string in the **Community string** box, then click **Save**.

### Notes

- Certain alerts assigned to groups of machines can simultaneously generate a large number of responses. For example, you can set the alert "Computer configuration change" and associate it with an e-mail action. If a software distribution patch is applied to those machines with this alert setting, it would generate a number of e-mails from the core server equal to the number of machines to which the patch was applied, potentially "flooding" your e-mail server. In this case, an option might be to handle this alert by simply writing it to the core log rather than send e-mail.

- Some alert actions do not affect device health. These include actions such as Run Program on Client, Shut Down/Restart, and any alert that is Informational only. However, if any of these actions are combined with other alert actions that do affect device health, then any alerts generated will affect device health and will appear in the alert log.
- When you select **Execute program on core**, programs do not display as expected on the core server's desktop. When the program is run, it is started as a service in Windows and so is not displayed as a regular application would be. Programs that are run in this way should not contain a user interface that requires interaction.
- The **From** field in an e-mail does not need to contain a valid e-mail address, but can contain text in the form of an e-mail address (user@domain.com) that describes the source of the alert or that is otherwise helpful to the e-mail recipient.
- SNMP traps identified as version 1 are processed, while those identified as version 3 are only forwarded.

## Configuring an alert ruleset

Use the **Alert configurations** page to create a new alert ruleset. Before you can configure alerts, you must configure actions. (See "[Configuring alert actions](#)" for more information.)

There are two alert rulesets that appear by default on the **Alert configurations** page:

- **Core alert ruleset:** this ruleset ensures that alerts are sent to the core server when the **Device monitor** feature is enabled (see [Monitoring for connectivity](#)). This ruleset can only contain one alert type, Device monitor. You can edit the status, action, alert action, and health settings only. If you attempt to make any other changes they will be ignored.
- **Default ruleset:** this ruleset is deployed to all managed devices and contains a number of alert types that are of general use for most network administrators. You can edit this ruleset to add other alert types and change the settings for the default alert types. Any time you edit this ruleset, the changes are deployed to all managed devices even if you do you explicitly redeploy the ruleset.

In addition to these rulesets you can create custom rulesets to apply to targeted groups of managed devices.

### To create an alert configuration

1. In the left navigation pane, click **Alerting**, then click the **Alert configurations** tab (if necessary).
2. Click **New**, type a name in the **Name** field, type a description of the alert in the **Description** field, then click **OK**.
3. Click the configuration you just named, and click **Edit configuration**.
4. Click **New**.

5. In the **Alert type** drop-down list, select the component, action, or event type you want to receive alerts on.
6. Check each status you wish to alert on: **Informational**, **OK**, **Warning**, or **Critical**. For example, to receive an alert if the type you selected in step 5 crosses a critical threshold, check **Critical**.
7. In the **Action** drop-down list, select the action you want to occur if the conditions specified in steps 5 and 6 are met. These actions are defined beforehand; if you want an action that is not in the list, you can [create](#) one using the **Action configurations** page.

---

Certain alerts assigned to groups of machines can simultaneously generate a large number of responses. For example, you can set the alert “Computer configuration change” and associate it with an e-mail action. If a software distribution patch is applied to those machines with this alert setting, it would generate a number of e-mails from the core server equal to the number of machines to which the patch was applied, potentially “flooding” your e-mail server. In this case, an option might be to handle this alert by simply writing it to the core log rather than send e-mail.

---

8. In the **Action configuration** drop-down list, click the configuration. There may only be one configuration available (the contents of this list change depending on what you selected in step 7).
9. Check **Affects device health** if you want the alert to apply to the server's health state when it is displayed in the dashboard or the **All devices** list. If the severity level for the alert is **Informational** only, the alert will not affect device health.
10. Click **Add**.
11. Repeat steps 5-10 to add additional alerts to the ruleset.
12. When finished, click **Close**.

To edit an alert configuration, select the configuration (step 3) and click **Edit configuration**, then continue with the steps above.

A few minutes after you create or edit a configuration, the configuration deployment service automatically attempts to update all computers that previously had that configuration deployed to them. Or, if you want to deploy the configuration immediately, click the **Deploy configuration** tab and click **Deploy**.

## Deploying configurations

Use the **Deploy configurations** page to move the selected alert to targeted devices. First, you should target the devices you want to send the alert configurations to.

### To deploy configurations

1. In the left navigation pane, click **My devices**, then click the **All devices** group.
2. Select the devices to which you want to deploy the alert configuration, then click **Target** to place the devices in the **Targeted devices** list.
3. In the left navigation pane, click **Alerting**, then click the **Deploy configuration** tab.

4. In the **Alert configurations** box, select the alert you want to deploy.
5. Click the link to view the **Targeted devices** list. To remove a device from this list, right-click it, then click **Remove**. To add devices, you must add them to the [targeted list](#).
6. Click **Deploy** to deploy the selected configuration to the targeted devices.

As part of the deployment process, an XML page is created that lists the deployed configurations and devices the configurations were deployed to. This report is saved on the core server in the LDLOGON\ALERTRULES directory, and is named with a sequential number assigned by the database. If you want to view this XML page separately from deploying a configuration, click the **Generate XML** button and then click the link to view the XML file.

## Viewing alert configurations for a device

Use the **Alert configurations** page to view a list of the alert configurations assigned to the selected device, and to view the details of each alert.

### To view alert configurations

1. In the **My devices** view, click the device you want to configure.
2. In the **Properties** page, click **View details**.
3. In the left navigation pane, click **Alert configuration**.

The following details are provided about each alert. For more information on modifying these details, see [Using alerts](#).

- **When state reaches:** When the state of the alert reaches the displayed state, an alert will be generated.
- **Rule name:** The name of the alert ruleset, as defined in the [Alert configurations](#) dialog.
- **Action configuration:** The action that occurs when the alert is generated, as defined in the [Action configurations](#) dialog.
- **Alert type:** The kind of alert to be generated, such as an e-mail, an SNMP trap, or executing a program.
- **Alert handler:** The handler associated with the alert, such as an e-mail handler.

## Viewing the alert log

Use the **Alert log** page to view alerts sent to the core or to managed devices. The log is sorted by Time (GMT), the most recent being at the bottom of the log.

The Alert log contains the following columns:

- **Alert ID:** The unique identification number of the alert (as generated by sequentially by the database).
- **Time:** The date and time the alert was generated (GMT).
- **Alert name:** The name associated with the alert, as defined in the **Alert configurations** page.
- **Status:** The status of the alert. The status is a number, and the number represents one of the following:
  - **0 Unknown:** The status cannot be determined.

- **1 Informational:** Supports configuration changes or events that manufacturers may include with their systems.
- **2 OK:** Indicates that the status is at an acceptable level.
- **3 Warning:** Provides some advance warning of a problem before it reaches a critical point.
- **4 Critical:** Indicates that the problem needs your immediate attention.
- **Instance:** Indicates the specific source of the alert.
- **Device name:** The name of the server on which the alert was generated.
- **IP address:** The IP address of the server on which the alert was generated.

#### To view the global alert log

1. In the left navigation pane, click **Alerting**.
2. Click the **Alert log** tab.
3. Select an alert and click **Clear alert** to clear the health status of the alert, click **Delete entry** to delete the log entry, or click **Purge log** to empty the log.

#### To view the alert log for a specific device

1. Double-click the device in the **My devices** list.
2. In the left navigation pane, click **System information**.
3. Click **Logs**, then double-click **Alert log**.
4. To list log entries by name, status, or instance, click the **Filter** button on the toolbar and select the filter criteria. For example, select **Alert name** and type a complete name (such as Performance) or a partial name with the \* wildcard (such as Remote\*).
5. To view log entries for a range of dates, clear the **Show events for all dates** check box and select a range of dates.
6. Click **Find** on the toolbar to view the alerts associated with the filter options you chose.

# Vulnerability scanner

---

LANDesk technology includes a vulnerability scanning tool that lets you update known vulnerability definitions, download associated patches, scan managed devices for vulnerabilities, and remediate affected devices by deploying and installing the appropriate patches.

Read this chapter to learn about:

- [Vulnerability scanning overview](#)
- [Understanding and using the Scan Vulnerabilities window](#)
- [Configuring devices for vulnerability scanning](#)
- [Updating vulnerability definitions](#)
- [Viewing vulnerability and detection rule information](#)
- [Purging vulnerability information](#)
- [Scanning devices for vulnerabilities](#)
- [Viewing detected vulnerabilities](#)
- [Downloading patches](#)
- [Remediating vulnerabilities](#)

## Vulnerability scanning overview

The vulnerability scanner tool helps you establish ongoing patch-level security on the managed devices across your network. You can automate the repetitive processes of maintaining current vulnerability information, assessing vulnerabilities for the various operating systems running on your managed devices, downloading the appropriate patch executable files, remediating vulnerabilities by deploying and installing the necessary patches on affected devices, and verifying successful patch installation.

This product uses LANDesk's standard role-based administration to allow users access to the Scan vulnerabilities tool. Role-based administration is LANDesk's access and security model that lets LANDesk Administrators restrict access to tools and devices. Each user is assigned specific rights and scope that determine which features they can use and which devices they can manage. A LANDesk Administrator assigns these rights to other users with the Users tool in the console. The role of vulnerability scanning and remediation is represented by a corresponding right, called Patch Manager, in role-based administration. This right appears in the User Rights/Scopes dialog. In order to see and use the vulnerability scanner tool, a user must be assigned the necessary Patch Manager right. Additionally, for remediation, a user must have the core functionality right. The Patch Compliance right provides users with the ability to add and remove security definitions from the Compliance group and change the status of definitions contained in the Compliance group. The right does not allow for the editing of custom definitions or security threat's custom variables. To use Vulnerabilities, you must be logged in as a user with the Patch Manager, Basic Web console, Reports, and Patch compliance rights.

The vulnerability scanner works with the management gateway, but remediation does not work..

You will be able to view Apple<sup>\*</sup> and Sun<sup>\*</sup> definitions, but you will not be able to push these definitions to devices because this product does not have agents that support these operating systems.

Vulnerability scanning supports most of the standard server platforms, enabling you to scan for vulnerabilities and deploy security patches to managed servers running the following operating systems:

### Supported server platforms

- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4
- Windows 2000 Professional SP4
- Windows 2003 Standard Edition SP1
- Windows 2003 Enterprise Edition SP1
- Windows XP Pro SP2
- RedHat Enterprise Linux ES/AS 3
- SUSE Linux Server 9 (Professional, Enterprise, and Advanced)

For information on configuring your managed devices for vulnerability scanning and patch deployment, see [Configuring devices for vulnerability scanning](#).

## Understanding and using the Scan Vulnerabilities window

Users with the Patch Manager right will see the Vulnerabilities tool in the console's left navigation pane. When you click Vulnerabilities, the vulnerability scanning features appear in the console window, as described below:

The vulnerabilities window contains a toolbar and two panes. The left pane shows a hierarchical tree view of vulnerability groups. Click on a group to view its contents in the right pane. The right pane displays vulnerability definition details in a column list. At the top, it contains a Find button to quickly search for the specified criteria. In the Find box, the following extended characters are not supported: < , > , ' , " , !.

### Toolbar buttons

- **Update:** Opens the Update Vulnerabilities Settings dialog where you can specify the source site, platforms, and languages whose vulnerability information you want to update. You can also configure whether to place vulnerabilities in the Enabled (or Scan) group, whether to download associated patches concurrently, the location where patches are downloaded, and proxy server settings.
- **Schedule download:** Opens the download task in the Scheduled Task dialog where you can configure task options. When you click Save, the download task is placed in the Scheduled tasks window and under the Vulnerability Tasks tab.
- **Schedule security tasks:** Opens the Schedule Vulnerability Scan dialog where you can provide a name and configure scanner options.
- **Refresh:** Updates the list in the right pane with the latest downloaded vulnerability information.
- **Purge:** Opens the Delete Vulnerabilities dialog where you can specify the platforms and languages whose vulnerability information you want to remove from the core database.

### Left pane (tree view)

The left pane of the window shows the following groups:



- **Scan:** Lists all of the vulnerabilities that are searched for when the vulnerability scanner runs on managed devices. In other words, if a vulnerability is included in this group, it will be part of the next scan operation; otherwise, it won't be part of the scan.

Scan can be considered one of three vulnerability states, along with Don't Scan and Unassigned. As such, a vulnerability can reside in only one of these three groups at a time. A vulnerability is either Scan, Don't Scan, or Unassigned and is identified by a unique icon for each state (question mark (?) icon for Unassigned, red X icon for Don't Scan, and the regular vulnerability icon for Scan.) Moving a vulnerability from one group to another automatically changes its state.

To move vulnerabilities from one group to another, right-click the vulnerability and select the group to move the vulnerability to.

By moving vulnerabilities into the Scan group, you can control the specific nature and size of the next vulnerability scan.

New vulnerabilities can also be automatically added to the Scan group during an update by checking the **Put new definitions in the Scan group** option on the **Update Vulnerabilities Settings** dialog.

---

#### **Caution about moving vulnerabilities from the Scan group**

When you move vulnerabilities from the Scan to the Don't Scan group, the current information in the core database about which scanned devices detected those vulnerabilities is removed from the database and is no longer available in either the Vulnerability Properties dialog or in the scanned Server Information dialog. To restore that vulnerability assessment information, you would have to move the vulnerabilities back into the Scan group and run the scan again.

---

- **Do not Scan:** Lists the vulnerabilities that aren't searched for the next time the vulnerability scanner runs on devices. As mentioned above, if a vulnerability is in this group, it can't be in the Scan or Unassigned group. You can move vulnerabilities into this group to remove them from a vulnerability scan.
- **Detected:** Lists all of the vulnerabilities detected by the previous vulnerability scan, for all of the target devices included in that scan job. The contents of this group are always determined by the last vulnerability scan, whether one device was scanned or many devices.

The Detected list is a composite of all detected vulnerabilities found by the most recent scan. The Scanned and Detected columns are useful in showing how many devices were scanned, and on how many of those devices the vulnerability was detected. To see specifically which servers have a detected vulnerability, right-click the definition then select **View affected computers**. Note that you can also view vulnerability information for a specific server in its [Server information console](#) dialog.

You can only move vulnerabilities from the Detected group into either the Unassigned or Don't Scan groups.

- **Unassigned:** Lists all of the vulnerabilities that do not belong to either the Scan or Don't Scan groups. The Unassigned group is essentially a holding area for collected vulnerabilities until you decide whether you want to scan for them or not.



By default, collected vulnerabilities are added to the Scan group during an update.

You can move vulnerabilities from the Unassigned group into either the Scan or Don't Scan groups.

- **View by OS:** Lists all of the downloaded vulnerabilities organized into specific device operating system subgroups. These subgroups help you identify vulnerabilities by OS category. You can use these OS subgroups to copy a set of vulnerabilities into the Scan group for OS-specific scanning.

Vulnerabilities can be copied from an OS group into the Scan, Don't Scan, or Unassigned group. Vulnerabilities can reside in more than one platform and/or product group simultaneously.

- **View by Product:** Lists all of the downloaded vulnerabilities organized into specific product subgroups. These subgroups help you identify vulnerabilities by product category. You can use these product subgroups to copy vulnerabilities into the Scan group for product-specific scanning.

### Right pane (list view)

The right pane of the window displays the following vulnerability details, listed in sortable columns:

- **ID:** Identifies the vulnerability with a unique, vendor-defined alphanumeric code.
- **Severity:** Indicates the severity level of the vulnerability. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown.
- **Title:** Describes the nature or target of the vulnerability in a brief text string.
- **Language:** Indicates the language of the OS affected by the vulnerability.
- **Date Published:** Indicates the date the vulnerability was published by the vendor.
- **Silent Install:** Indicates whether the vulnerability's associated patch file installs silently (without user interaction). Some vulnerabilities may have more than one patch. If any of a vulnerability's patches don't install silently, the vulnerability's Silent Install attribute says No.
- **Repairable:** Indicates whether the vulnerability can be repaired through patch file deployment and installation. Possible values are: Yes, No, and Some (for a vulnerability that includes multiple detection rules and not all detected vulnerabilities can be repaired).

Double-click the vulnerability ID to view more detailed information on its properties dialog. From a vulnerability properties dialog, you can see the detection rules for the vulnerability, download associated patch files, and click the rule to view its detailed properties dialog.

## Configuring devices for vulnerability scanning

Before managed devices can be scanned for vulnerabilities, and receive patch deployments, they must have the vulnerability scanner agent installed.

The easiest way to deploy the vulnerability scanner agent to multiple managed devices is to create a new agent configuration, with the vulnerability scanner agent selected (default setting), and then schedule the configuration for the desired target devices with Scheduled tasks.

When you configure a device to support vulnerability scanning, the necessary files for vulnerability scanning, and remediation (i.e., patch deployment and installation) are installed on the target device.

## Updating vulnerability definitions

Your network is continuously vulnerable to security threats from new worms and viruses, as well as ordinary maintenance issues like software updates and bug fixes. New hardware and software is released every day, along with the patches to repair inevitable vulnerabilities. The vulnerability scanning tool makes the process of gathering the latest known vulnerability, detection rule, and patch information quick and easy by letting you update vulnerabilities via a LANDesk-hosted database. This security service consolidates known vulnerabilities from trusted, industry/vendor sources.

By establishing and maintaining up-to-date vulnerability and associated patch information, you can better understand the nature and extent of the security threats for each server operating system you support, determine which vulnerabilities are relevant to your network environment, and customize vulnerability scanning and remediation tasks. The first step is to keep up with the latest known vulnerability information.

You can configure and perform vulnerability updates at once, or create a scheduled vulnerability update task to occur at a set time or as a recurring task.

### To update vulnerability information

1. In the left navigation pane, click **Vulnerabilities**. (For a description of the dialog, see About the Update Vulnerabilities Settings dialog.)
2. Click the **Update** toolbar button.
3. Select the update source site from the list of available content servers.
4. Select the platforms whose vulnerability information you want to update. You can select one or more platforms in the list. The more platforms you select, the longer the update will take.
5. Select the languages whose vulnerability information you want to update for the platforms you've specified. You can select one or more languages in the list. The more languages you select, the longer the update will take.
6. If you want new vulnerability definitions (vulnerabilities that do not already exist in the database) to automatically be placed in the Unassigned group instead of the default location which is the Scan group, uncheck the **Put new definitions in the Scan Group** check box.
7. If you want to automatically download the actual patch executable files, check the **Download associated patches** check box, and then click one of the download options.
  - **For detected definitions only:** Downloads only the patches that are associated with vulnerabilities detected by the last vulnerability scan (i.e., the vulnerabilities that are currently residing in the Detected group).
  - **For all referenced definitions:** Downloads ALL of the patches that are associated with vulnerabilities currently residing in the Scan group. (this will take a long time)

Patches are downloaded to the location specified in the Patch Settings section of the dialog (see procedure below).

8. If you have a proxy server on your network that is used for external Internet transmissions (required to update vulnerability information and download patches), click **Proxy Settings** tab and specify the server's address, port number, and authentication credentials if a login is required to access the proxy server.
9. Click **Apply** at any time to save your settings.
10. Click **Update Now** to run the vulnerability update. The Updating Vulnerabilities dialog displays the current operation and status.
11. When the update has completed, click **Close**. Note that if you click **Cancel** before the update is finished, only the vulnerability information that has been processed to that point is downloaded to the core database. You would need to run the update again in order to obtain all of the remaining information.

---

**Note:** Do not close the console while an update vulnerability process is running or the process will be terminated. This does not apply to a scheduled download task.

---

#### To configure the patch download location

1. On the Update Vulnerabilities Settings dialog, tab over to the **Patch Settings** section.
2. Enter a UNC path where you want the patch files copied. The default location is the core server's \LDLogon\Patch directory.
3. If the UNC path entered above is to a location other than the core server, enter a valid username and password to authenticate to that location.

The folder must have file and web sharing enabled and Anonymous access must be enabled.

4. Enter a Web URL where servers can access the downloaded patches for deployment. The Web URL should match the UNC path above.
5. You can click **Test Settings** to check to see if a connection can be made to the Web address specified above.
6. If you want to restore the UNC path and Web URL to their default locations, click **Reset patch settings**. The default location is the core server's \LDLogon\Patch directory.

## Scheduling vulnerability downloads

You can also configure vulnerability updates as a scheduled task to automatically occur at a set time in the future, or as a recurring task. To do this, simply click the **Schedule download** toolbar button to open the Scheduled task properties dialog where you can name the task and configure its options. When you click **Save**, the task appears in the Scheduled tasks window.

All scheduled vulnerability update tasks will use the current settings found in the Update Settings dialog. So, if you want to change the source site, platforms, languages, patch download site, or proxy server settings for a particular update job,

you must first change those settings in the Vulnerabilities Update Settings dialog BEFORE the task is scheduled to run.

### To configure a Schedule download task

1. In the left navigation pane, click **Vulnerabilities**.
2. Click **Schedule download**.
3. On the **Schedule task** page, configure the [schedule](#).
4. Click **Save**.

When you click **Schedule download**, a task is created (it has no targeted devices, and it is unscheduled). If you cancel this Scheduled task procedure, please be aware that it has still been created and appears in the Task list.

## Viewing vulnerability and detection rule information

After vulnerabilities have been updated with the latest information from the LANDesk security service, you can view vulnerability lists in the console, view them by platform and product, and move the vulnerabilities into different status groups. For information on the different groups in the window and how to use them, see [Understanding and using the Scan Vulnerabilities window](#) earlier in this chapter.

To view vulnerability details, double-click a **Vulnerability ID** to open its Vulnerability Properties dialog (see About the Vulnerability Properties dialog). From this dialog you can also access detection rule details by double-clicking a patch file name in the Detection Rules list to open the Patch Properties dialog (see About the Patch Properties dialog).

This information can help you determine which vulnerabilities are relevant to your network's supported server platforms, how a vulnerability's detection rules check for the presence of a vulnerability, what patches are available, and how you want to configure and perform remediation for affected devices.

You can also view vulnerability definition and detection rule information specific to scanned devices directly from the console by accessing the local console from **My devices**, and clicking **Vulnerabilities** in the left navigation pane.

## Purging vulnerability information

You can purge vulnerability information from the vulnerabilities window (and subsequently from the core database) if you determine that it isn't relevant to your environment.

When you purge vulnerability information, associated detection rule information is also removed from the database. However, the actual patch executable files aren't removed by this process. Patch files must be removed manually from the local repository, which is typically on the core server.

### To purge vulnerability information

1. Click the **Purge** toolbar button. (For a description of the dialog, see About the Purge Unused Vulnerability Information dialog.)
2. Select the platforms whose vulnerability information you want to remove. You can select one or more platforms in the list.

If a vulnerability is associated with more than one platform, you must select all of its associated platforms in order for the vulnerability's information to be removed.

3. Select the languages whose vulnerability information you want to remove (associated with the platform specified above).

If you select a Windows platform above, you should specify which language vulnerability information you want to remove. If you select a UNIX platform above, you must specify the Language-neutral option in order to remove cross-language vulnerability information.

4. Click **Remove**.

## Scanning devices for vulnerabilities

Vulnerability assessment means checking the currently installed versions of operating system-specific files and registry keys on a device against the most current known vulnerabilities in order to identify security risks on your servers. After reviewing known vulnerability information (updated from industry sources) and deciding which vulnerabilities you want to scan for, you can perform customized vulnerability assessment on managed devices that have the vulnerability scanner agent installed. (For information on configuring devices for vulnerability scanning and patch deployment, see [Configuring devices for vulnerability scanning](#) earlier in this chapter.)

When the vulnerability scanner runs, it always reads the contents of the Scan group and scans for those specific vulnerabilities. Before scanning servers for vulnerabilities, you should always make sure only the vulnerabilities you want to scan for are included in that group. You can move vulnerabilities into and out of the Scan group to customize the size and nature of a vulnerability scan.

### Running the vulnerability scanner

The vulnerability scanner can be pushed to devices as a scheduled vulnerability scan task from the console.

### To create a vulnerability scan task

1. In the left navigation pane, click **Vulnerabilities**.
2. Make sure vulnerability definitions have been updated recently.
3. Make sure the Scan group contains only those vulnerabilities you want to scan for.

4. Click the **Schedule security tasks** toolbar button. (For a description of the dialog, see About the Schedule Vulnerability Scan dialog.)
5. Enter a unique name for the scan. If the task script already exists, you can select whether to overwrite the existing script.
6. Specify whether you want the vulnerability scanner to display a progress dialog on the target device. You can also specify whether you want a Cancel button to appear with the scanner dialog, so that the end user has the option of cancelling the scan.
7. Specify how you want the vulnerability scanner dialog to close when it is done running on target devices. You can require end user input, or you can set the dialog to close after a specified timeout period.
8. Click **OK**.
9. Select the task\* and set targeting and [scheduling](#) parameters, and click **Save**.

\*The vulnerability scan task appears in Vulnerability tasks.

## Viewing detected vulnerabilities

If the vulnerability scanner discovers vulnerabilities for any of the enabled vulnerabilities on any of the target devices, this information is reported to the core server and added to Detected list.

You can use any of the following methods to view detected vulnerabilities after running a vulnerability scan:

### By the Detected group

Select the **Detected** group in the vulnerabilities window to view a complete listing of all vulnerabilities detected by the most recent scan.

### By an individual device

Double-click a device name in My devices, and then click **Vulnerabilities** to view detailed vulnerability assessment information for that device.

## Downloading patches

In order to deploy security patches to devices with detected vulnerabilities, the patch executable file must first be downloaded to a local patch repository on your network. The default location for patch file downloads is the core server's /LDLogon directory. You can change this location in the Patch Settings section of the Update Vulnerabilities Settings dialog.

---

### Patch download location and proxy server settings

Patch downloads always use the download location settings currently found in the Patch Settings section of the Update Vulnerabilities Settings dialog. Also note that if your network uses a proxy server for Internet access, you must first configure the proxy server's settings in the Proxy Settings section of the Update Vulnerabilities Settings dialog before you can download patch files.

---

The product first attempts to download a patch file from the URL (shown on the Patch Properties dialog). If a connection can't be made, or if the patch is unavailable for some reason, the product downloads the patch from the LANDesk security service, which is a company-hosted database containing patches from trusted industry sources.

You can download one patch at a time, or a set of patches together at the same time.

### To download single patches

1. Double-click a vulnerability name to open its **Properties** dialog.
2. In the Detection Rules section, select the detection rule patch files you want to download, and then click **Download Selected Patches**.
3. The download operation and status displays in the Downloading Patches dialog. You can click **Cancel** at any time to stop the entire download process.
4. When the download is finished, click the **Close** button.

### To download multiple patches

All scheduled vulnerability update tasks will use the current settings found in the Update Settings dialog. So, if you want to change the source site, platforms, languages, patch download site, or proxy server settings for a particular update job, you must first change those settings in the Vulnerabilities Update Settings dialog BEFORE the task is scheduled to run.

1. In the left navigation pane, click **Vulnerabilities**.
2. Click **Schedule download**.
3. On the **Schedule task** page, configure the schedule.
4. Click **Save**.

## Removing patch files

To remove patch files, you must delete the files manually from the patch repository, which is typically on the core server.

# Remediating vulnerabilities

Once you've updated vulnerability definitions, put the vulnerabilities you want to scan for in the Scan group, run a vulnerability scan on managed devices, determined which vulnerabilities require attention, and downloaded the necessary patches, the next step is to perform vulnerability remediation by deploying and installing the necessary patches on target affected devices.

Vulnerability remediation is done on an individual vulnerability basis. In other words, you create a remediation task for a specific vulnerability that deploys and installs the necessary patch files.

Note that remediation, like vulnerability scanning, only works on devices that have been configured with the vulnerability scanner agent. For more information, see [Configuring devices for vulnerability scanning](#) earlier in this chapter.



Linux remediation is not supported, due to licensing issues. You can use the Vulnerabilities tool to discover vulnerabilities on Linux devices, then decide if you want to remediate the vulnerabilities. If you want to do so, you can use a Red Hat support subscription to download the necessary RPMs, then create a software distribution package to deploy the RPMs to devices.

---

**WARNING:** Many patches will automatically reboot the device upon completion.

---

#### To create a custom remediation script

1. In the left navigation pane, click **Vulnerabilities**.
2. Select the **Detected** group to view vulnerabilities detected by the most recent scan. (You do not have to select this group. If you want to create a custom remediation script for vulnerabilities that haven't been scanned for or haven't been detected yet, click any of the other vulnerability groups to view their contents and select a specific vulnerability.)
3. Right-click the definition then select **View affected devices** to view devices that have this vulnerability.
4. Right-click the definition then select **Create remediation task**.
5. (optional) Modify the name in the Task Name text box.
6. Select from the options, then click **OK**.
  - **Copy affected computers to the target cart:** Copies computers affected by the vulnerability to the target cart for remediation.
  - **Show progress when running:** Enables the scanner to display information on end user devices while it is running. Click this option if you want to show scanner activity, and if you want to configure other display and interaction options in this dialog. If you don't click this option, none of the other options on this dialog are available to configure, and the scanner runs transparently on devices.
  - **Allow user to cancel scan:** Shows a Cancel button on the dialog on the end user device. Click this option if you want the end user to have the opportunity to cancel a scan operation. If this option is not checked, the dialog doesn't have a Cancel button and the end user can't stop the scan.
  - **Require user input before closing vulnerability scan dialog:** Click this option if you want the scanner to prompt the end user before its display dialog closes on the device. If you select this option, and the end user does not respond the dialog remains open which could cause other scheduled tasks to timeout.
  - **Automatically close dialog after a timeout:** Click this option if you want the scanner's display dialog to close after the duration you specify.





# Remote server access

---

## About remote access

Use the remote control feature to easily resolve device problems from one location. Read this chapter to learn about:

- [Remote controlling devices](#)
- [Using remote control](#)
- [Configuring Windows 2003 client security for remote control](#)
- [Accessing remote Linux servers](#)

## Remote controlling devices

Remote control allows users to remotely diagnosis and troubleshoot many device problems. During a remote session, you can do anything at the remote computer that a user sitting at it could do while using the keyboard layout of your machine, not that of the target machine. All of your actions happen in real time on that computer. You can set remote control access through the Role-based administration tool. It allows you to:

- Fix software and hardware problems quickly by allowing authorized users to check and take control of a computer remotely
- Access remote files
- Transfer files in either direction
- Execute remote applications
- Remote reboot

## Using remote control

To use remote control from the console, you must first install the remote control viewer. You need administrative privileges on the local computer to install the viewer, which you are prompted to download the first time you access the remote control page. If necessary, you can uninstall the remote control viewer using the Windows Control Panel's Add/Remove Programs applet. Look for **LANDesk Server Manager Remote Control Console** in the program list. The remote control agent also must be installed on each remote device you want to control.

### To remote control a device

1. In the dashboard, right-click the icon of the device you wish to connect to and select **Remote control**, which will launch the viewer.

or

In the console, right-click the device you wish to connect to and select **Remote control**, which will launch the viewer.

2. In the Administrative console, single-click the device and select the **Remote control**, **SSH**, or **SFTP** button in the **Properties** tab in the lower pane

or

Double-click to launch the local console and click **Remote session** in the left navigation pane.

You can also remote control more than one computer at a time. After starting one session, return to the dashboard or console and select another computer.

To be remote-controlled, Windows servers must have the LANDesk remote control agent installed and loaded. This agent is installed by

- Creating an agent configuration task in the console and scheduling a deployment to the device, or
- Mapping a drive from the device to the core server and running the appropriate agent configuration.

This agent may be loaded as a resident service in order to provide immediate access to the machine, or it may be installed as an on-demand agent that loads only when needed.

Additionally, you can install the remote control mirror driver to improve the performance of detecting, capturing, and compressing screen changes if the server CPU is slower (< 2.0GHz) or the network is fast (> 100mpbs). Note that remote control doesn't support DOS graphics or full-screen DOS windows. The command prompt window may not display initially when using the mirror driver. If this occurs, minimize the window then maximize it.

To access a Linux device remotely, at least the standard LANDesk agent must have been deployed to that device. After clicking that device in the **My devices** list, you have a choice of SSH and SFTP on the lower pane. Select either option to launch a new window. Note that if the device has not had any agent deployed yet, double-clicking that device in the **My devices** list and selecting **Remote session** will launch the Windows viewer as a default behavior, as the OS is not yet known. The viewer will report that it was unable to connect to the client.

## Configuring Windows 2003 client security for remote control

The resident service uses Windows NT security. To work with Windows 2003 servers, you must configure the server clients so that the Windows 2003 sharing and security model for local accounts is classic (local users authenticate as themselves). If you don't do this, the default guest-only authentication won't work with remote control's Windows NT security.

### To set the Windows 2003 security model to classic

1. On the Windows 2003 client, click **Start | Control Panel**.
2. In the **Administrative Tools, Local Security Policy** applet, click **Security Options > Network access: Sharing and security model for local accounts**, and set it to **Classic - local users authenticate as themselves**.

## Controlling remote Windows devices

### To start remote control

1. In the administrative console's **All devices** group, or from within one of your groups, click the device you want to control.
2. Select **Remote control** in the **Properties** tab in the lower pane to launch the viewer.

Or

3. Double-click the device you want to control and click **Remote session** in the left pane.

Once you've taken control of a remote device, its screen appears in the **Viewer** window with Autoscroll enabled. If the remote control agent is loaded, the **Session messages** window in the viewer tells you that the agent is found and what protocol it's using.

### To use hot keys

1. You must be actively remote controlling a device to use hot keys.
2. With the focus on the **Viewer** window, press the hot key combination for any one of the available actions.

The available hot keys are found in the **Special key** icon on the toolbar. You may also change the default mappings.

### About the Viewer window focus

If you find that the hot keys don't work, the focus isn't on the **Viewer** window. If the border is blue/black, the focus isn't on the window. Click inside the window to change the border to yellow/black. You should now be able to use hot keys.

### To view different areas of a remote device screen

By default the Autoscroll option is enabled. When enabled and currently remote controlling a device, you can place your cursor along the yellow/black border of the **Viewer** window and scroll up, down, or side to side. The closer your cursor gets to the border, the faster the scrolling will occur. If you wish, you can disable Autoscroll in the **Options** menu. You can then use the **Move remote screen** icon. Your cursor will become a hand that you can click, drag, and release to view various areas of the remote screen.

## Viewing connection messages

You can use the **Viewer** window's connection messages section to view a history of status messages sent to the status bar (such as remote control agent package exchanges). In addition to the other information this history contains, it lets you:

- Diagnose problems with the session

- Check whether the remote control agent is loaded
- Check the status of the remote control agent

### To view connection messages from the console

1. In the **Viewer** window, click **View**, and click **Connection messages**.

## Saving connection messages

While you're in a remote control session, you have the option of saving the connection messages. These messages may be useful as an audit trail or if you need to troubleshoot any issues related to using remote control on a particular device.

### To save connection messages

1. In the **Viewer** window, click **File**, and click **Save connection messages**.
2. In the **Save As** dialog, type in a file name and save as a .TXT file. The connection messages are saved to the My Documents folder by default.

If the remote control agent is loaded, the **Session messages** window tells you that the agent is found and what protocol it's using. You will also see a magnifying glass icon appear on the server you selected.

## Executing programs remotely

In the **Viewer** window, you can start any program on a remote device to diagnose issues.

### To execute programs remotely

1. In the toolbar's **Run** field, enter the path for the program you want to run. If you need to browse the program, click the drop-down list and select **Browse**.
2. To run the program on the remote device, click the **Remote execute** icon to the left of the **Run** field.

## Transferring files to remote devices

You can use the remote control **Viewer** window to transfer files to and from your machine and the remote device. In essence, this works as though you've mapped a drive to the remote device. You can only transfer files to/from devices that have the remote control agent installed. This feature works even if you're not currently remote controlling a device as long as the connection has been created. The **Run each Explorer window in a separate process** option doesn't work with file transfer.

To transfer files to a device

1. Click **Tools | File transfer**. Windows Explorer appears.
2. Select a file to transfer by clicking the filename. Right-click the file and select **Copy**, or select to drag and drop.

3. Scroll down the Windows Explorer tree to **Remote Computers**. Below this you should see the name of the remote device you're controlling. Select a folder to paste the file to, then right-click and select **Paste**.

Similarly, you can also transfer files from a remote device to your device.

## Shutting down and rebooting remote devices

You can remotely shut down or reboot devices. When you do, a message box appears on the remote device with a warning that the system will shut down in 10 seconds. If someone is currently at that machine they can click a **Shutdown** or **Cancel** button. If no action is taken the reboot will happen when the countdown reaches 0. When typing a time before rebooting the device, the maximum number of seconds allowed is 300 seconds (five minutes).

If the device has applications open with unsaved data, those applications will probably interrupt the shutdown when they prompt for the user to save. You may have to remote control the device and save/close applications for the shut down or reboot to work.

## Configuring session options

Use items under the **Options** menu to enhance the quality of a remote control session. You can speed up the viewing rate and change the **Viewer** window settings.

In the **Change settings** tab:

- **Autoscroll**: Set by default. Enables the **Viewer** window to scroll as you move the cursor closer to the window border. Toggle on/off; item is on when a check mark appears next to it.
- **Keyboard and mouse lockout**: Locks the server's keyboard and mouse so that only the user running the **Viewer** window can control the remote server. Toggle on/off; item is on when a check mark appears next to it. Note that special key combinations in Windows such as "CTRL-ALT-DEL" or the "Windows Key+L" aren't locked out.
- **Synchronize clipboards**: Set by default. Synchronizes the keyboards between the **Viewer** console and the remote server so you can paste information between the two machines. Toggle on/off; item is on when a check mark appears next to it.
- **Blank server screen**: Blanks the server's screen so only the user running the viewer can see the user interface display on the remote server. Toggle on/off; item is on when a check mark appears next to it.

In the **Optimize performance** tab:

Optimize performance for: Select Modem, Broadband, LAN, or custom as appropriate for your network environment

**Display:**

- **Use the mirror driver**: Loads the mirror driver for enhanced performance on slower machines. Toggle on/off; item is on when a check mark appears next to it.
- **Suppress the wallpaper**: Speeds up the viewing rate by suppressing the remote device's background wallpaper. Ornate wallpapers can substantially slow down a remote control session. Toggle on/off; item is on when a check mark appears next to it.

- **Color depth reduction:** If you're connecting via a slow link or Dial-up Networking connection, this option reduces the amount of transferred color information. The closer you move the slider to full reduction, the more color artifacting you might see.

## Mirror driver

During the Server Manager installation, you had the option to install the remote control mirror driver. This driver can reduce the amount of time required to see the target machine's desktop and increase the visual quality of the targeted desktop's image. A raster-based approach to screen capture can be implemented without any drivers, which is a huge advantage if the agent is to be downloaded over the Internet or installed on machines by users who do not have administrative rights. However, significant performance improvements can be achieved by using a driver that receives all of the output that Windows is sending to the real display driver.

## Accessing remote Linux devices

To access a Linux server remotely, at least the standard LANDesk agent must have been deployed to that server. After clicking that Linux device in the **My devices** list, you have a choice of **SSH** and **SFTP** in the lower pane. Selecting either option will launch a new window.

Note that if the server has not had any agent deployed yet, double-clicking that device in the **My devices** list and selecting **Remote session** will launch the Windows viewer as a default behavior, as the OS is not yet known. The viewer will report that it was unable to connect to the client.

If you select SSH access, a window opens with an SSH session on the remote server. You must provide a username and password to access the server. When you have authenticated, a secure shell session opens on the remote server.

If you select SFTP access, a window opens with a secure FTP view of the remote server (based on an SSH connection). You must provide a username and password to access the server. When you have authenticated, you can use the secure FTP functionality to transfer files between your computer and the remote server.

# Software distribution

---

## Software distribution overview

The Software distribution tool gives you the ability to distribute software packages to target devices. The tool supports many different types of packages. Software distribution consists of these main steps:

1. **Create or obtain a software package.** The software package can be one or more MSI files, an executable, a batch file, RPM files (Linux), or a package created with LANDesk's package builder. If the software package is a batch file, see "Using the Start command in a batch file package" below. In most cases, the software package needs to contain everything necessary to install the application you're distributing. Put the package on your delivery server.
2. **Create a distribution package.** The distribution package contains the files and settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, command-line switches, and so on. These settings are stored in the database and create a "distribution package." Once you create a distribution package, the information is stored in the database and can easily be used in multiple tasks.
3. **Create a push delivery method.** The push delivery method defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Don't create a delivery method every time you want to distribute a package. Delivery methods allow you to define best practices for deploying software. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.
4. **Schedule the distribution job in the Scheduled tasks window.** Here you specify the distribution package, the delivery method, the devices that need to receive the distribution package, and when the task should run.

When the scheduled time occurs, the scheduler service will start the scheduled task handler which contacts the software distribution agent on each device and informs it that the package is ready for installation.

The software distribution agent then obtains the package from the delivery server and processes it on the device by installing or removing the packaged files.

After the package is processed, the software distribution agent sends the result to the core server, where it's recorded in the core database.

Separating distribution tasks into two parts, distribution packages and delivery methods, simplifies the distribution process. Now you can create delivery method templates that are independent of a particular package. If you have different people in your organization that create packages and distribute packages, these changes help simplify job roles and task divisions. Package creators can now work independently from package deliverers.

Software distribution enables you to deploy software and file packages to devices running the following operating systems:

- Windows 2000
- Windows 2003



- Windows XP
- Red Hat Enterprise 3 Linux AS and ES
- SUSE LINUX Server 9 (Advanced, Enterprise, and Professional)

Devices receiving the software distribution packages must have the following LANDesk agents installed:

- Standard LANDesk agent
- Software distribution agent (Windows only)

Software distribution features include:

- Delivery methods enable detailed control over how tasks complete
- Easy task scheduler integrates with the inventory database to make target selection easy
- Real-time status reporting for each deployment task
- Full-featured package builder to build complete software packages
- Ability to distribute any package type, including MSI, setup.exe, and other installers

If you don't have an existing package that you want to deploy, you can use LANDesk's package-building technology to create a standalone executable program for the required software installation. A Web server or network server can be configured as a "delivery server" to store distribution packages. Through the console, you can schedule the distribution task. The core server communicates the package's location (URL or UNC path) to the device, and the device then copies only the files or the portions of the files it needs from the delivery server.

For example, if you're reinstalling a previously deployed software program because some of its files were corrupted or missing, the system copies only the damaged or missing files, not the entire program. This technology also works well over WAN links. You can store the package on multiple servers, and then schedule devices to use the server appropriate to their needs (that is, location proximity, bandwidth availability, and so on).

## Using the Start command in a batch file package

The batch file distribution package has been designed to run as if it were issued from the Run command in the Windows Start Menu. When a batch file is executed using the Run command, it closes upon completion. A program that is required to run in an open command window will close prematurely when run through a batch file distribution package.

The program can be configured to continue running by using the "Start" command in the batch file. The "Start" command will actually spawn a new command window that remains open after the batch file has completed and closed the initial command window.

Here is an example of a batch file that uses the "start" command to spawn a new command window running the Sample.exe program.

```
start "Title" /D "c:\program  
files\ManagementSuite\ldclient\sdmcache\swd\alertttest" Sample.exe
```

The first parameter ("Title") is the name of the command window that will be displayed in the title bar. Note that the title is mandatory because the path to the

executable will be misinterpreted as the Title if it is omitted. If the path to the executable includes a space, it must be in quotes. If the title were not present, the quoted path to the file would be mistaken for the title, even though the /D switch indicating the path is present.

This single line batch file runs Sample.exe in a new command window titled "Title." For more help on the Start command, type the command with either the /h or /? switch at a command prompt.

## Setting up a distribution package delivery server

The delivery server is the server that stores the software distribution packages. It can be either a Web server or a Windows NT/2000/2003 server. We recommend that for best results the packages be URL-based. In general, properly configuring a URL is less work than configuring a UNC path.

### Delivery Requirements server

Web server	Microsoft Internet Information Server 5.0 or higher running on Windows NT or Windows 2000/2003, or any HTTP 1.1 compliant Web server with byte range support.
Network server	Windows NT 4.0 or Windows 2000/2003

## Configuring Windows Web servers for software distribution

### To configure a Microsoft IIS 5.0 Web server for software distribution

These steps explain how to create a virtual directory on a Web server and enable it for browsing. In general, virtual directories need to allow reading and directory browsing and anonymous access to the virtual directory must be enabled. Execute must not be set or the share won't work correctly. You also may want to disable write permissions so devices can't change the directory's contents.

1. Create a directory on the Web server where you want to store your software distribution packages. The usual location for such a directory on an IIS Web server is a subdirectory in the c:\inetpub\wwwroot directory.
2. Copy the packages to this directory.
3. From the **Control Panel**, double-click **Administrative Tools** and then **Internet Services Manager**.
4. In the right panel, double-click the icon with the device's name and then click **Default Web Site**.
5. In an empty area in the right panel, right-click and select **New**, then click **Virtual Directory**.
6. From the wizard, click **Next** and then enter an alias for your directory. Click **Next**.
7. Either enter the path or browse to a path and click **Next**.
8. In the **Access Permissions** dialog, enable **Run script** and **Browse**. This enables you to browse packages when creating the software distribution script. Click **Next** and **Finish**.

9. To enable **Port 80** on the Web server, in the left panel, right-click **Default Web Site**.
10. Click **Properties**. In the **Web Site Identification** dialog, the **TCP Port** box should display 80. If it doesn't, click **Advanced** to add the port.
11. Ensure that the Web site is available by opening a browser and entering the URL for your Web server and virtual directory. For example, if the name of your Web server is Test and the name of the virtual directory is Packages, enter the following URL:

`http://Test/Packages`

A list of the packages you have copied to this directory should appear.

The size and number of packages you put in this directory is limited only by available disk space. Subdirectories can be created to logically group packages. Each subdirectory that's created must have the above access permissions set.

Once you copy the packages to a package share on a Web server, they're staged and ready to be copied to the target devices. When scheduled, the URL or UNC path of the package is passed to SDCLIENT.EXE (the device agent) as a command-line parameter. SDCLIENT.EXE manages the file transfer, starts the installation, and reports the status. Although the HTTP protocol is used for the file transfer, the status report is returned through the standard LANDesk agent.

The Web server communicates with the device to ensure that the package copies correctly. If the package transmission is interrupted during the download, the Web server can use the HTTP protocol to restart the download at the point where it stopped. The Web server doesn't check, however, to ensure that the package was installed correctly. That traffic is TCP-based, and it returns the status to the core server using the standard LANDesk agent.

### To configure a Microsoft IIS 6.0 server for software distribution

Windows 2003 Server handles virtual directories differently than Windows 2000. On a Windows 2003 server, if you select a directory and from its shortcut menu make it a Web share, the directory registers itself in IIS 6 as a Web application rather than a virtual directory. The problem is that as a Web application, when an executable file is selected, the Web server attempts to run the file as a Web application rather than download the file to the user. The resolution is to go into IIS, change the shared directory from a Web application to a virtual directory, and turn off execute permissions.

### Linux packages information

When hosting RPM files for Linux on a Windows server, files without a registered MIME file type will fail to execute unless you do the following.

### To register MIME file types

1. Launch Internet Information Services (IIS) Manager.
2. Expand the local computer in the tree.
3. Click **Web Sites > Default Web Site**.
4. From the package Web share's shortcut menu, click **Properties**.
5. Click the **HTTP Headers** tab.

6. Click **File Types** on the **MIME Map** section.
7. Click **New**.
8. In the **Associated Extension** box, type **.RPM**.
9. In the **Content Type (MIME)** box, enter **text/plain**.
10. Click **OK** twice and apply the changes.

## Configuring a network server for software distribution

Devices that don't have a browser must receive distribution packages from a UNC path on a Windows NT/2000/2003 network server. This can be the same folder as the one you set up on your Web server. For UNC path-based distributions to work correctly, you must enable a null-session share folder on your network server. Use the SYSSHRS.EXE utility to create a null-session share folder.

1. To set up a shared folder on your network server, right-click the folder you want to share and then click **Sharing**.
2. Click **Share this folder** and click **Permissions**.
3. Add the appropriate file rights such that
  - **Core (Task Scheduler user):** Access at deployment time (when the package is deployed).
  - **Console (Logged-in user):** Access while creating the package to browse for a file or check SWD packages and MSI packages to verify they contain unique IDs.
  - **Target (null session):** Uses a null-session share to read the package.

One simple method to accomplish this is to give the Everyone group and the Guest and Anonymous accounts read rights.

4. The Everyone group needs file access rights to the files within the share. To do this, click **Security**, click the **Everyone** group, and click **Read & Execute**, **List Folder Contents**, and **Read permissions**.
5. From your network server, click **Start | Run** and browse to the LDMAIN\Utilities folder on your core server.
6. Run the **SYSSHRS.EXE** utility.

**Note:** Although this utility states that it's for Windows NT devices, it also works on Windows 2000/2003 devices.

7. Check the shared folder you set up and click **Apply** and then **Close**.
8. Copy the software distribution packages to this folder on the network server.

Additional steps needed to configure a Windows Server 2003:

9. Open the Group Policy Object Editor by clicking **Start | Run**, and typing "gpedit.msc". Right-click **Network access: Let everyone permissions apply to anonymous users**, click **Properties**, and select **Enable**.
10. In the Group Policy Object Editor, right-click **Network access: Restrict anonymous access to Named Pipes and Shares**, click **Properties**, and select **Disable**. The policy just below it must contain the name of the share that is to be the null session share.

The size and number of packages you store on the network server is limited only by the available disk space.

For more information about the SYSSHRS.EXE utility, download the SHARES.EXE package from <http://www.LANDesk.com/support/downloads/Resource.aspx?pvid=12&rtid=10> and extract the documentation.

## Distributing software to Linux devices

Once you've deployed the Linux agents, you can distribute software to your Linux devices. The initial Linux agent deployment uses an SSH connection. Once the agents are installed, the core server uses the standard LANDesk agent to communicate with the Linux server and transfer files. To distribute software to a Linux device, you must have Administrator rights.

You can only distribute RPMs to Linux devices. The Linux agents will automatically install the RPM you distribute. The RPM itself isn't stored on the server after installation. You can install and uninstall the RPM you specify using software distribution. You can only use push delivery methods with Linux software distribution. For Linux software distribution, the settings in the push delivery method are ignored, so it doesn't matter which push delivery method you select or what the settings in it are.

The distribution follows this process:

1. The core server connects to the Linux device through the Standard LANDesk agent
2. The device downloads the package
3. The device runs a shell script that uses RPM commands to install the RPM package
4. The device sends status back to the core server.

You can store Linux RPMs on HTTP shares. Linux software distribution doesn't support UNC file shares. For HTTP shares, make sure you've enabled directory browsing for that share. If you use an HTTP share on a Windows device other than the core, you need to configure IIS with the correct MIME type for RPM files. Otherwise, the default MIME type IIS uses will cause the RPM to fail to download the file.

### To configure the RPM MIME type on Windows devices

1. From Windows **Control Panel**, open **Internet Services Manager**.
2. Navigate to the folder that hosts your distribution files. From that folder's shortcut menu, click **Properties**.
3. On the **HTTP Headers** tab, click the **File Types** button.
4. Click **New Type**.
5. For the **Associated Extension**, type **rpm**. Note that rpm is lower-case.
6. For the **Content type**, type **text/plain**.
7. Click **OK** to exit the dialogs.

Once you've hosted the files on your package share, create a new Linux distribution package, associate it with the delivery method you want, and schedule the delivery.

## Distribution file descriptions

This is a list of the files used in SWD, as well as descriptions of how they work together. You can use this information to customize how packages are created, stored, and deployed in your organization.

These files are installed at the core server:

- ManagementSuite\CUSTJOB.EXE
- ManagementSuite\SDMAKINI.DLL
- ManagementSuite\LANDesk.ManagementSuite.WinConsole.dll
- ManagementSuite\INSTALL\EN\_PKG\_BLD\SETUP.EXE
- ManagementSuite\LDLOGON\SDCLNSTL.EXE

These files are installed at the device:

- C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE
- sdistexh.dll
- sdistmsi.dll
- ldapinfo.dll
- C:\Program Files\LANDesk\LDClient\AICLIENT.DLL
- C:\Program Files\LANDesk\LDClient\SDMCACHE (this is an empty folder)
- C:\LDCLIENT.LOG (this file is created by the SDCLIENT.EXE file)
- INST32.EXE
- EUNINST32.DLL (or other locale-specific resource file)
- %WINDIR%\aiclient.log
- %WINDIR%\inst32.log
- %DEST%\WebPortal\WebPortal.exe
- %DEST%\WebPortal\SDClientMonitor.exe
- %DEST%\WebPortal\style.css
- %DEST%\WebPortal\img\LANDesk\_logo.jpg
- %DEST%\WebPortal\img\logo.jpg
- %DEST%\WebPortal\img\SWDPortalTitle.jpg
- %DEST%\WebPortal\img\title1.gif
- ldredirect.dll
- sdcln.dll
- sdmsi.dll

## File descriptions

**SETUP.EXE:** This standalone, binary installation file is used to create package-building computers, placing the Package Builder, Package Builder wizard tools, and accompanying online help files onto the computer. Each application that you package with Package Builder is made into a self-extracting .EXE.

If you're using the Web Console, you must copy the .EXE to the packages folder on your Web server for users to access.

SETUP.EXE installs the following types of files on the package-building computer in the Program Files\Intel\Package Builder folder:

- BUILDER.EXE: Enhanced Package Builder executable

- **ENUBLDR.DLL:** Enhance Package Builder resource file
- **REPLICATOR.EXE:** Package Builder wizard executable
- **ENUREPLC.DLL:** Package Builder wizard resource file
- **BASIC.CFG:** A simple installation script for building a software distribution package
- **TYPICAL.CFG:** A more complex installation script for building a software distribution package
- **ENUBLDR.HLP:** Help file for the Package Builder
- **ENUBLDRI.HLP:** Help file for the Package Builder wizard

**CUSTJOB.EXE:** This file is launched directly by the scheduler when a job is to begin.

**SDC\_INSTALL.INI:** This job script is processed by CUSTJOB.EXE. It copies SDCINSTL.EXE to a remote device and then executes it on that device via the standard LANDesk agent (CBA). This file is placed in the DTM\Scripts folder.

**SDCLNSTL.EXE:** This file installs the SWD client files SDCLIENT.EXE and AICLIENT.DLL on Windows 95/98 and Windows NT/2000/2003/XP devices. This file is placed in the DTM\LDLogon folder on the core server.

**SDCLIENT.EXE:** This file is ultimately placed on the device in the C:\Program Files\LANDesk\LDClient folder. It's invoked with command-line parameters that include the URL or UNC path of the distribution package to be installed. This invocation is normally a result of the core server Scheduler calling CUSTJOB.EXE.

**SDISTEXH.DLL:** Handles the installation and removal of packages built by the LDMS 6.3 and earlier package builder.

**SDISTMSI.DLL:** Installation/removal library for Microsoft Installer (MSI) packages.

**AICLIENT.DLL:** This file is called by SDCLIENT.EXE; it's copied to the same folder as SDCLIENT.EXE.

**INST32.EXE:** This is the actual installer program. It's embedded within every self-extracting package. It's also installed into the LDClient folder and launched by SDCLIENT.EXE whenever a request to install a software package is received.

**ENUINST32.DLL:** This is a locale-specific resource file, and its name varies with the locale.

**AICLIENT.LOG:** This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to AICLIENT.LOG1. When the new AICLIENT.LOG file exceeds the 50 KB limit, AICLIENT.LOG1 is renamed to AICLIENT.LOG2. It's incremented one more time to AICLIENT.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current AICLIENT.LOG file.

**INST32.LOG:** This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to INST32.LOG1. When the new INST32.LOG file exceeds the 50 KB limit, INST32.LOG1 is renamed to INST32.LOG2. It's incremented one more time to INST32.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current INST32.LOG file.

**WEBPORTAL.EXE:** This CGI-based portal communicates through the local client's Standard LANDesk agent and checks with the local software distribution cache for policies that apply to the local device/user. The portal then displays a Web page listing available policies. All the files in the WebPortal folder pertain to this application.

**REDIRECT.DLL:** Aids in the support of redirecting file download to a specified preferred package server.



## About Distribution packages

The **Distribution packages** view shows the available distribution types and any packages you've created for each distribution type. When you select a distribution package you've created, you can view the properties for it, delete it, clone it, or reset the package hash.

To create a new distribution package, select a distribution package type in the toolbar and click **New**.

For more information on software distribution, see "[Software distribution overview](#)." For more information on the distribution package dialog options, see "Distribution packages and delivery methods dialog help."

## Understanding the distribution package types

Software distribution supports these package types:

### MSI

These are packages in the Windows Installer format. You must use a third-party tool to create MSI packages. These packages consist of a primary .MSI file and can include supporting files and transforms. Transforms customize how MSI packages are installed. If your MSI package consists of multiple files, make sure you add all of them as additional files in the Distribution package dialog.

### Software distribution packages (SWD)

These are packages built with the Management Suite Package Builder (installed separately).

### Executables and batch files

These types of packages will run if the command was issued from a DOS prompt. Add command line options in the Distribution packages dialog.

### Linux

The product supports Red Hat Linux ES and AS, and SUSE Linux Server 9 (Enterprise, Professional, and Advanced). RPM deployment is supported. Scripting is not supported. Additional files need to be in a location where Linux can reach them. A Web share or an anonymous HTTP site can be used to store RPMs. Linux does not support mapped drives.

## Package Groups

**My packages:** Packages that the current user has created. The administrative users can also see these packages.

**Public packages:** Packages that users have marked common. Anyone who schedules a package from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group



for that user.

**All packages:** Both the current user's packages and packages marked public.

**User packages:** (administrative users only) List of all packages sorted by owner/creator (not including public packages).

## Resetting package hashes

The software distribution agent uses the MD5 hash algorithm to verify the package and additional files are downloaded correctly. When a distribution package is first scheduled, the product downloads the files and calculates the hash values associated with the primary file and any additional files used by the distribution package. If the hash stored with the package doesn't match the hash value the agent computed on the target device, the download isn't considered valid. If you make any changes to the package outside of this product, such as updating the package contents, you need to reset the hash, or any scheduled tasks using the updated package will fail.

## Cloning

Cloning creates a duplicate of an existing package, such as a package that delivers an executable to a set of targeted devices. If the settings of the package are what you want for another package that will deliver a different executable, you would select the package you want to clone, click **Clone**, and change the executable to be delivered.

## About the Scheduled tasks tab

Distribution includes a powerful scheduled task system. Both the core server and managed devices have services/agents that support scheduled tasks. The Server Manager console can add tasks to the scheduler.

A task consists of a distribution package, delivery method, targeted devices, and a scheduled time.

Use the **Scheduled tasks** tab to configure and schedule scripts you've created. Schedule items for single delivery, or schedule a recurring task. For information on the fields, see [Scheduled tasks](#).

Before you can schedule tasks for a device, it must have the standard LANDesk agent and be in the inventory database. LANDesk Server configurations are an exception. They can target a server that doesn't have the standard LANDesk agent.

### To schedule a distribution task

1. In the left navigation pane, click **Distribution**.
2. Click **New** to create a package.
3. Click the new package and click **Schedule**.
4. Configure a [distribution package](#) and a [delivery method](#).
5. On the **Target devices** page, select the query you created that targets the devices you want. You can also target devices in the target cart by clicking **Add target list**. Targeted devices appear in the lower box.
6. On the **Schedule task** page, configure the [schedule](#).
7. Click **Save**.

When you click **Schedule**, a task is created (it has no targeted devices, and it is unscheduled). If you cancel this Scheduled task procedure, please be aware that it has still been created and appears in the Task list.

## About the Delivery methods tab

The **Delivery methods** tab shows you the available delivery methods and any delivery methods that you've configured. When you select a delivery method you've created, you can view the properties for it, delete it, or clone it. The product only supports the Push delivery method. A default push delivery method is created during installation.

To create a new delivery method, click the **New** button.

### Delivery method groups

**My delivery methods:** Delivery methods that the current user has created. The administrative users can also see these delivery methods.

**Public delivery methods:** Delivery methods that users have marked common. Anyone who schedules a delivery method from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group for that user.

**All delivery methods:** Both the current user's delivery methods and delivery methods marked public.

**User delivery methods:** (administrative users only) List of all delivery methods sorted by owner/creator (not including public delivery methods).

For more information on software distribution, see [Software distribution overview](#).

### To create a new delivery method

1. In the left navigation pane, click **Distribution**.
2. In the lower pane, click the **Delivery methods** tab, select a delivery method type from the left pane, and click **New**.
3. Use **Description** to add descriptive text about the delivery method and change the owner if you want.
4. In the left pane, select other pages from which to select options. The **Discovery** page is used to verify the target computer is configured properly to accept the distribution package.
5. When finished, click **Save**.

### About the Description page

Use this page to describe the delivery method you're creating and to set the number of devices you want to distribute to simultaneously.

- **Owner:** Allows users to share methods by setting them to the public owner.
- **Delivery method name:** The name for your delivery method.
- **Description of delivery method:** The description you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer names.

## About the Reboot page

Use this page to configure whether the computer is rebooted after the software has been installed or removed. You have three options:

- **Never reboot:** Devices won't reboot after a package installation. If you select this setting and your package requires a reboot, devices may encounter errors running the application until they do reboot. If the package is an SWD package, this option overrides any settings in the package. If the package is a generic executable or an MSI package, the package setting may override this option.
- **Reboot only if needed:** Devices will reboot if the package requires it.
- **Always reboot:** Devices will reboot regardless of whether the package requires it or not.

## About the Discovery page

This page allows you to choose options for device discovery. Before the scheduled task handler can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

Discovery options:

- **UDP:** Selecting UDP uses a Ping Discovery Service (PDS) ping via UDP. Most Server Manager device components depend on PDS, so your managed devices should have PDS on them. PDS is part of the standard LANDesk agent. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping retries and timeout.
- **TCP:** Selecting TCP uses an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Number of retries:** The number of attempts discovery makes to contact devices.
- **Discovery timeout:** The number of milliseconds before discovery retries will timeout.
- **Timeout for subnet broadcasts:** The number of milliseconds before subnet broadcast retries will timeout.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast. When selected, this will result in a subnet directed broadcast being sent via UDP using PDS.
- **DNS/WINS:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

## Understanding distribution error codes

When a distribution job finishes, the **Scheduled tasks** page will either display success or an explanation of why it failed. In addition, each targeted client has log files that contain information about the distribution. The status and errors are logged to the following files:

- If the error occurred while attempting to access the package, the error is logged in the AICLIENT.LOG file.

- If the error occurred while processing the package (for example, copying files), the error is logged in the INST32.LOG file.
- The SDCLIENT.LOG file contains general summary information about each installation request received from the core server.

These log files are stored on each client. The following table lists the error codes you may encounter in these files.

<b>Error code</b>	<b>Definition</b>
101	The user cancelled the install.
102	File access was denied.
103	The password used isn't valid.
104	No network found, or incorrect path provided.
105	A download error occurred.
106	A socket could not be created.
107	Unable to open an HTTP session.
108	A CFG download error occurred.
109	A save CFG error occurred.
110	No save CFG folder exists.
111	A file access error occurred.
112	A get CFG error occurred.
113	Unable to create a backup CFG.
114	A spawn error occurred because another package is already being installed.
117	The backup directory can't be created.
180	Networking error. Can't initialize.
188	Timed out while downloading over HTTP.
189	HTTP connection aborted.
191	Host not found.
197	HTTP file not found.
201	The UNC file cannot be found.
202	The file was not found on the installation disk.
203	Unable to create a file in the specified location.
204	Not enough disk space on the destination drive for installation.
205	An invalid drive was specified, or the drive required for this install was not available.
206	The file has a long filename and can't be installed by the 16-bit install program. You still have the option to continue to install other files.
207	The specified file is not an executable.
208	Multiple uninstall registry entries exist with the same source path.
209	Unable to locate the uninstall executable.

210	Encountered an invalid compressed file, or HTTP error(s).
211	A successful AFXSOCKETINIT command must occur before using this API.
212	The network subsystem failed.
213	No more file descriptors are available.
214	The socket can't be created. No buffer space was available.
215	The specified address was already in use.
216	The connection attempt was rejected.
217	The provided host address was invalid.
218	The network can't be reached from this host at this time.
219	The attempt to connect timed out without establishing a connection.
220	The virtual circuit was aborted due to a timeout or other failure.
221	The virtual circuit was reset at the remote site.
222	A non-stated HTTP error occurred.
223	An HTTP error occurred; the file wasn't open for reading.
224	An HTTP error occurred; no content-length setting provided.
225	An HTTP error occurred; not enough memory available.
226	A memory allocation error occurred.
227	Unable to read the file.
228	Insufficient memory available.
229	The .CFG file has an error at line XX.
240	The temporary path specified is invalid. It can't be accessed or created. The target computer has a configuration problem.
301	This application has never been installed on this computer; it can't be uninstalled.

## Troubleshooting distribution failures

Software distribution provides the ability to distribute packages to a large number of devices at once. If there is a problem with the package, or the software being deployed conflicts with already existing software, you have the ability to cause problems at thousands of devices at once. When planning a deployment using software distribution, take care to not overwhelm the help desk.

Before deploying a new package, test it with some test systems. Ideally, these test systems should include all of the operating systems and applications that are used in your environment. Once the package is deployed, confirm that all of the systems and applications are still working as expected.

Once the package has been validated against test systems, do a limited deployment. Target a small number of devices in your environment. When deciding how many devices to target, the rule of thumb is not to target more devices than your help desk can handle. Once the package has been deployed to these devices, test the system for a couple of days to see if users encounter any problems.

After the initial deployment, you can begin rolling out the software to other devices in the enterprise. The speed at which these roll out occurs should be based upon how much device variety the enterprise has and how much of a load the help desk can handle.

Here are some other problems you might encounter:

Software distribution provides the ability to distribute packages to a large number of devices at once. If there is a problem with the package, or the software being deployed conflicts with already existing software, you have the ability to cause problems at thousands of devices at once. When planning a deployment using software distribution, take care to not overwhelm the help desk.

Before deploying a new package, test it with some test systems. Ideally, these test systems should include all of the operating systems and applications that are used in your environment. Once the package is deployed, confirm that all of the systems and applications are still working as expected.

Once the package has been validated against test systems, do a limited deployment. Target a small number of devices in your environment. When deciding how many devices to target, the rule of thumb is not to target more devices than your help desk can handle. Once the package has been deployed to these devices, let the software sit for a couple of days to see if users encounter any problems.

After the initial deployment, you can begin rolling out the software to other devices in the enterprise. The speed at which these roll outs occur should be based upon how much device variety the enterprise has and how much of a load the help desk can handle.

Here are some other problems you might encounter:

### **Scheduled task can't find package**

If the scheduled task indicates that the package can't be located, make sure that the package can be viewed from the device.

If the package is URL-based, you can check to make sure it is accessible by using a Web browser. Remember, if your DNS is set up to resolve the package, you'll need to verify that the package has been distributed to all of the Web servers.

If the package can be viewed from the device but still does not download properly, the problem may be that the URL or UNC based package share doesn't allow anonymous access. Check the permissions on the UNC or URL share and make sure it allows anonymous access. For UNC locations, make sure it has properly been configured as a null session share.

### **Bandwidth detection doesn't work**

One of the most common problems that can occur is having PDS set up for bandwidth detection. In device setup, one of the common base agent options is to choose between PDS and ICMP for device bandwidth detection. When a device is configured to use PDS for bandwidth detection, it will only detect between RAS and non-RAS connections. So, if you configure a distribution to only work with high speed connection and the package installs on a computer with a WAN connection, check and make sure it is configured to use ICMP and not PDS.

# Scripting

---

## Scripting overview

The Package Builder wizard steps you through the process of creating a software distribution package. The wizard saves the commands required to perform the same installation on other computers. It writes these commands to an ASCII file with a .CFG extension. You can edit this script file after creating it in Package Builder, or you can create one from scratch and build it into a package.

The Package Builder online help provides syntax information for each of the script commands. To access the help for a specific command, highlight a command in the left panel and press the **F1** key.

To access a specific script file, start Package Builder and click **File | Open**.

Once a script has been modified, click **Build | Build** to build the script into a package.

## Script commands

Each script includes two sections. Specific commands at the top of the script define the operating parameters, and the balance of the commands describes the installation of the application included in the software distribution package.

All of the commands included in a script can be grouped into one of these functional categories:

- Base Installation
- Appearance
- Messages & Input
- System Changes
- If Conditions
- Defaults & Calls

These categories contain related commands that describe the installation process for each package. Some commands describe the operating parameters of the installation and must be placed at the top of the script file. For details about each command, see the Package Builder online help.

## Editing packages with the Package Builder

The Package Builder interface is divided into three areas:

- In the left pane, the functional categories are listed. Expand each functional category to display the individual commands within that category.
- The right pane is divided into two screens: The upper portion displays the script itself. The lower portion is a GUI template that contains entry boxes for the parameters of the highlighted command.

To see the details of a command in the script, highlight the command and view the parameter details in the lower portion of the screen.

To add a new command to the script, select the location in the script where the command should be located. Next, highlight the command in the left pane. Now complete the syntax template in the lower portion of the screen. When you've selected the command parameters, click **Add** to insert the new command.

## Using scripting commands

### Don't pass variables to the DLL Load command in Package Builder

If you create a package that depends on passing a variable into the DLL Load command, it won't work if the variable doesn't arrive at the correct time. If the .DLL doesn't receive the expected variable, the package won't complete the installation correctly. To avoid this problem, don't pass variables into the DLL Load command; the other DLL parameters work correctly.

### Using the Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands

The Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands require the full path to the executable to run correctly. Also, the RunAtMiddle command must be positioned in the script after the DEFAULTDIR function to work correctly. RunAtStart and RunAtExit commands can be anywhere in the script and will run correctly.

### Rebooting during package creation

When using the Package Builder wizard to create a package, you may be prompted to reboot the package-building computer. In many cases, rebooting before completing the package-building process causes the package to improperly install at the client. The application becomes configured for the package-building computer rather than the targeted client. However, in some cases, the reboot is required because the installation program accesses the installation CD after reboot.

You need to test the resulting package to determine whether you can stop the installation process and create the package before the reboot, or whether you need to reboot the package-building computer during the software installation and then continue to create the package.

## Creating and naming software distribution packages

### Package names can't be changed once they're created

You can't change a package name once you complete the package creation step. If you attempt to directly change the filename, your users can't access that package correctly.

### Package names can't include hyphens or periods

If you use hyphens or periods in a package name, the package-creation process will truncate the name when it encounters them. You can still access the package in a



script, and users can install it, but the truncated name might be confusing. Don't use hyphens or periods in a package name. You can use the underscore (\_) character instead.

We recommend that you create a new working directory each time you begin creating a package. To create this directory, start the Package Builder wizard, and click **Scan Options**. In the Temporary Work Directory box, either type in the full path to a directory or browse to its location. Package Builder prompts you for permission to create a directory that does not already exist.

### Store only software distribution packages in your distribution location

You should only keep packages in the Web server location or UNC folder that you set up for software distribution. If you store other types of executable files in this folder, they may be confused with packages when you're creating distribution package scripts. If you create a distribution script for an executable that's not a package, the distribution will fail. Store only software distribution packages in your distribution location.

For more information about creating and modifying packages, see the topic "Working with the Package Builder" in the Package Builder online help.

### File collections can't contain more than 296 files

When you create a file collection package, you can add as many as 296 separate files or folders. If you attempt to add more than 296 items, the file collection stops. Files contained in an included folder count as one item, not as separate files.

### Simple sample script

This script contains some of the commands used to install Package Builder on a package-building computer. Major sections or commands are described with remarks (REM).

```
REM This is the Package Builder installation
REM Set screen graphics environment
SCREENCOLOR: (0,0,255), (0,0,255)
ANIMATION: "W:\Software\Install\Intel\duck\DISK01.BMP",
"W:\Software\Install\Intel\duck\DISK02.BMP",
"W:\Software\Install\Intel\duck\DISK03.BMP",
"W:\Software\Install\Intel\duck\DISK04.BMP",
"W:\Software\Install\Intel\duck\DISK05.BMP",
"W:\Software\Install\Intel\duck\DISK06.BMP",
"W:\Software\Install\Intel\duck\DISK07.BMP",
"W:\Software\Install\Intel\duck\DISK08.BMP",
"W:\Software\Install\Intel\duck\DISK09.BMP",
"W:\Software\Install\Intel\duck\DISK10.BMP",
"W:\Software\Install\Intel\duck\DISK11.BMP",
"W:\Software\Install\Intel\duck\DISK12.BMP",
"W:\Software\Install\Intel\duck\DISK13.BMP"
SCREENGRAPHIC: "W:\software\INSTALL\Intel\OAKLAN~1.BMP", topleft
REM TITLE: "LANdesk Management Suite", fontsize=25, color=yellow
REM SUBTITLE: "Package Builder", fontsize=18, italic, color=yellow
REM Configure uninstallation options
```

```

UNINSTALL: yes, removegroup, packagename="Package Builder"
UninstallBeginPrompt: "Do you wish to remove the LANdesk Management
Suite Package Builder programs and directories from your system?"
UninstallEndPrompt: "LANdesk Management Suite Package Builder programs
and directories have been successfully removed from your system."
REM Check for sufficient disk space before installation
IF DISKSPACE() < 4000K
BEGINFIRSTSCREEN caption="Not Enough Disk Space", Package Builder
requires 4 MB of disk space. Please arrange your hard disk so that a
sufficient amount of disk space is available.
ENDFIRSTSCREEN
REM This is only shown if there is less than 4 MB of disk space.
ENDIF
REM Define splash screen text
BEGINFIRSTSCREEN caption="LANdesk Management Suite Package Builder",
This installation program will set up LANdesk Management Package
Builder onto your hard disk. Contact your LANdesk Software Customer
Support representative if there are problems setting it up on your
computer.
ENDFIRSTSCREEN
REM Define default directory from which to work. Notice the variable
$ProgFilesDir$ comes from a Windows system environment variable. The
DEFAULTDIR command must be used before any file commands are used.
DEFAULTDIR: "$ProgFilesDir$\Intel\Package Builder", prompt="Please
enter the drive and directory:", caption="Directory Name", text="The
software will install onto your system in a directory. Please accept
the suggested directory location or type in one of your own. Make
certain to provide both a drive letter and the directory name."
REM Add files common to all versions of Package Builder. Only one has
been included in this sample script.
FILE: "CTL3D.000", overwrite=yes,
From="W:\Software\Install\Intel\CTL3D.DLL"
REM Install registry information
BEGINREGISTRY
KEY: new, "HKEY_CLASSES_ROOT\CFG"
VALUE: reg_sz, replace, "Default", "txtfile"
ENDREGISTRY
REM Setup Windows menu items
WINITEM: "LANdesk Management Suite", "$DEFAULTDIR$\Builder.exe",
"Package Builder", replace, allusers
WINITEM: "LANdesk Management Suite", "$DEFAULTDIR$\Replicator.exe",
"Package Builder wizard", replace, allusers
WINITEM: "LANdesk Management Suite", "$DEFAULTDIR$\ENUBLDRI.hlp",
"Package Builder wizard help", replace, allusers
REM Define and display final screen
BEGINLASTSCREEN caption="LANdesk Management Suite Package Builder",
The installation of the Management Suite Package Builder is now
complete.
ENDLASTSCREEN

```

## Sample script with more complex commands

This next script is organized into sections with a brief explanation for each. Any applications launched by a RunAtStart or RunAtMiddle command must be closed for the script to continue processing.

The beginning section of this script enables you to include a window title, package name, animated or still graphics, and audio, as well as color and font selections. A RunAtStart command enables you to execute an external application at the beginning of the installation.

Next, the BeginFirstScreen command enables you to inform the user about the installation by displaying a text message. Finally, the Backup command indicates that any files that are to be replaced will be backed up, and the OverWriteFile command indicates that the user will be prompted before any existing files are overwritten.

```
ANIMATION: "C:\WINDOWS\CIRCLES.BMP", "C:\WINDOWS\CARVED~1.BMP",
"C:\WINDOWS\BUBBLES.BMP", "C:\WINDOWS\BLUERI~1.BMP",
"C:\WINDOWS\BLACKT~1.BMP"
RUNATSTART: "c:\program files\accessories\mspaint.exe"
TITLE: "Package Builder Functionality Script for Windows 98", bold
INTROSCREEN: "C:\WINDOWS\SETUP.bmp", waittime=5, full
INTROSOUND: "C:\WINDOWS\MEDIA\START.WAV"
SCREENCOLOR: magenta, yellow
SCREENGRAPHIC: "C:\WINDOWS\PINSTR~1.BMP", topleft
FONTNAME: "Tahoma"
BEGINFIRSTSCREEN title="First Screen", caption="Screen #1"
This is the text that appears on the first screen.
ENDFIRSTSCREEN
BACKUP: YES
OVERWRITEFILE: ask
```

The following examples show different prompt options. Text for each prompt can be modified.

```
CancelPrompt: "Cancel?"
CopyFilePrompt: "UPLOAD IN PROGRESS"
OkPrompt: "GOOD JOB"
QuitPrompt: "Do you really want to quit?"
CopyTitlePrompt: "Copying..."
NextPrompt: "Next"
BackPrompt: "Back"
NoPrompt: "No"
YesPrompt: "Yes"
```

This section runs an external application and waits for that application to be closed before continuing. When the script continues, the user is prompted for input. Based on the selected option, the application continues and copies a file on the local drive or exits.

```
RUNATMIDDLE: "c:\windows\calc.exe"
ASK1: Yesno, caption="Sample question.", text="This is an example using
Yes / No buttons. Choose `Yes' to continue, `No' to exit."
IF $ASK1$= "yes"
WINGROUP: "New Program Group", prompt="Select a group",
caption="Program Group selection", text="Please select a program
group."
ELSE
IF $ASK1$= "No"
EXITMESSAGE
Sorry you had to leave so soon!
EXIT
ELSE
```

```

ENDIF
ENDIF
PROGRESSBAR: 302K
COPY: "C:\windows\setup.bmp", "C:\windows\temp\p1.bmp"
RENAME: "C:\windows\temp\p1.bmp", "C:\windows\temp\renamed p1.bmp"

```

This section launches an application as the last command before the script is completed. The RunAtExit command does not have to be the last line of the script.

This section also places a shortcut on the desktop and creates an uninstall package.

```

RUNATEXIT: "C:\WINDOWS\CDPLAYER.EXE"
BEGINLASTSCREEN title="Last screen", caption="The last screen"
This should be the last screen you see.
ENDLASTSCREEN
SHORTCUT: "c:\windows\notepad.exe", "NOTEPAD",
dir="c:\windows\desktop\"
UNINSTALL: yes, makeicon, removegroup, packagename="Package Builder
Functionality"

```

## Package Builder

### Running the Package Builder wizard

As described earlier, building a software distribution package is a two-phase process. The first phase creates an installation script (.CFG file) in the Package Builder working directory. This script contains all the client instructions for installing the software. The second phase builds the software distribution package. The package contains the instructions plus the files.

#### To run the Package Builder wizard

1. From your package-building computer, click **Start | Programs | LANDesk Management | Package Builder wizard**.
2. Click **Scan options** to configure the scan process. On this page, you can select which directories the wizard monitors for changes and whether the wizard creates a backup to return the client to its present state after the package has been created. When you're finished modifying the form, click **OK**.

---

#### At least one logical or physical disk drive must be monitored

The Package Builder wizard needs to monitor at least one logical or physical disk drive to track system information changes. If you clear the default drive selection in the **Scan options** page, and set it to monitor no drives, the wizard will exit.

---

3. Click **Build options** to configure user-specific settings for Windows NT and Windows 2000/2003/XP systems. You can select to have these settings applied to the logged-in user (or the default user if no one is currently logged in) or to all users. These user-specific settings include Start Menu items, shortcuts, and registry settings for the HKEY\_CURRENT\_USER key. To return, click **OK**.
4. Click **Next**. The wizard will check out your system.

5. Select the method you want to use to install the application:
  - If the installation program is locally available (such as a SETUP.EXE program), click **Browse** to locate the installation program, select it, and then click **Monitor**.
  - If the installation program is on an autorun CD, click **Next** and insert the CD.
  - To make other types of changes for a software distribution package (such as copying files or creating desktop shortcuts), click **Next** and run the appropriate utility.
6. Follow the prompts to install the software.
7. When the installation is complete, enter a name for the package. We suggest you enter a name that includes both the software and the operating system; for example, WinZip\_Win2K for a package that installs WinZip on a Windows 2000/2003 client.
8. Click **Compare**.
9. When the .CFG file has been created, click **OK** and then **Build**.  
**Note:** The .CFG file can be customized and then built into a package.
10. When the build completes, the wizard will put the package in the Onefile folder of the Package Builder Working directory. The package will be an .EXE file with the name you selected. Click **Finish**. You can manually test this package by clicking the .EXE file.

The next task is to set up the delivery server and copy this package to it.

## Setting up a package-building computer

The package-building computer should be a dedicated computer with a clean installation of its operating system. The clean installation is necessary because the package-building process captures all elements added or modified on the package-building computer.

Because you can distribute packages only to clients running the same operating system as the package-building computer, you should have a separate package-building computer, or a separate drive partition, for every operating system you distribute to. You can also use a single computer with multiple OS images as your package-building computer.

Any preinstalled software on the package-building computer reduces the Package Builder's ability to recognize changes. For this reason, your package-building computer must be as generic and clean as possible. This rule also applies to the CONFIG.SYS and AUTOEXEC.BAT files and other configuration files that the application installation process may modify.

### To install the package-building software

1. From your package-building computer, browse to ENUSETUP.EXE in the LDMAIN\install\Package\_Builder folder of the core server.
2. Double-click **ENUSETUP.EXE**, then click **Next**.
3. Type in the location of the folder where you want to install the package-building software, then click **Finish**.

Setup puts three items on the package-building computer:

- **Package Builder wizard:** Used to automatically create software distribution packages. It takes a "before" snapshot of the computer's state, has you install the software, takes an "after" snapshot of the computer's state, and builds a package from the differences in the snapshots.
- **Enhanced Package Builder:** Used to manually create, modify, and edit software distribution packages.
- **Package Builder wizard help:** Online help that describes the Package Builder wizard.

Once the Package Builder software is installed on your computer, you can use this computer to create and edit software distribution packages. The Package Builder stores packages on the local hard disk by default. Once these packages are built, you must move them from the package-building computer to the package share on your delivery server.

## Building a package

You can use the Package Builder wizard to automate the process of taking snapshots and compiling them into standalone packages. As shown below, the process includes four steps:

1. Taking a pre-installation snapshot
2. Installing the application or making a computer configuration change
3. Taking a post-installation snapshot
4. Restoring the package-building computer

### 1. Taking a pre-installation snapshot

To build a software package, use the Package Builder to scan the local hard drive. You can specify exactly which portions of the drive are scanned in the Scanning Options page. This scan checks the system registry and all the directories and files on the local computer. After you install new software on the system, the Package Builder uses this information to detect what changes were made to the computer; it then compiles these changes to create the software distribution package. This information is stored in the temporary work directory. Specify this directory in the Scan Options page of the Package Builder wizard.

Package Builder scans all local drives by default. If you don't plan to make any changes to a local drive during the installation, remove it from the scan to speed up the pre-scan process. For best results, allow the Package Builder to scan the drive partition where the operating system is stored, plus the drive where you intend to install the software or change the configuration.

If, at any time during the package-building process, the hard drive space on the package-building computer gets low, the Package Builder will stop, display a warning, allow you to provide more drive space, then continue the package-building process.

Even if you remove all the local drives from the scan list, the Package Builder still scans the system files and folders, as well as the computer's registry.

## 2. Installing the application or making a computer configuration change

Once the pre-installation snapshot is created, the Package Builder prompts you to install the application software to distribute as a package.

You can install multiple applications in a single package, but you should install only suite-type applications with this process. If you install multiple applications as one distribution package and later want to omit one, you must first remove the entire group and then install a new group of applications. If you want to install multiple packages to your managed clients, you should edit the software distribution script so that it installs several different packages during the distribution.

The Package Builder monitors the installation during this step, then waits until the installation is finished to continue with the wizard pages. You can then customize the finished program. For example, if the install program creates an uninstall icon that you prefer not to distribute to clients, you can delete the icon before the post-installation snapshot in step 3, omitting it from the package. You can also add new icons to specific program groups, which provides a single point of access for all your users.

You need to provide any setup information requested by the system, and answer all questions presented during the software setup. The Package Builder cannot perform these tasks for you, but it will save the information as part of the package.

If you want to change only some of the system settings on clients, or if you want to copy a collection of specific files, you can create a package without using the snapshot process.

When you're satisfied that the application software or the configuration changes are ready, return to the wizard and click Next to start the post-installation snapshot.

## 3. Taking a post-installation snapshot

In this step, the Package Builder takes a second snapshot of the package-building computer and compares it with the pre-installation snapshot. By analyzing the differences, the Package Builder can identify any changes that have occurred on the computer, and then build a package distribution configuration script. This file has a .CFG file extension, and is located in the c:\Program Files\LANDesk\Package Builder\ folder on the package-building computer.

This .CFG script file describes the changes to the registry, the file system, the desktop, and other system resources. It does not create a removal control file however, so you must add an uninstall option manually, either when you edit the script or when you schedule it for distribution.

Once these changes are saved, the Package Builder wizard offers the option to compile the .CFG file into an executable file, or to open it in Package Builder to make additional changes. Click Edit to open the new .CFG file in Package Builder and make your modifications. When you're satisfied with the installation, click Build to create the package.

Once finished, a page appears showing that the package was created and stored in the default directory on the package-building computer.

## 4. Restoring the package-building computer

Once you finish the package-building session, you should restore the package-building computer to its pre-installation state. This process ensures that the computer is in a clean state for the next package build. SWD doesn't include a process for restoring the computer to a clean state; therefore, you should use a computer-imaging program such as the LANDesk imaging tool that is part of OS Deployment, Symantec's Ghost\*, and so on to restore the client's operating system.

If you use a utility like Ghost to restore the package-building computer, you will also delete the .CFG file that was used to create the package. If you want to keep these files available, either to use in future packages or to edit at a later time, you can store them on a network share drive. Just specify a network location in the Scan Options page of the wizard to preserve these files.

By default, each new system scan is stored in a new working directory, but you can use the same folder again if you prefer to overwrite the old system scan. Some users keep software images of multiple operating systems on a single package-building computer. This solution provides optimum flexibility when creating software packages, without dedicating multiple computers specifically for software package building.

### Launching a package from a package

You can specify INST32.EXE on the command line of a RunAtExit command in one package in order to launch another package. The syntax is:

```
RunAtExit "INST32.EXE PACKAGENAME.EXE"
```

If the package is found on the network, this is more efficient than just running "PACKAGENAME.EXE." It allows you to specify a package name via an HTTP path. For example:

```
http://myservername/packages/PACKAGENAME.EXE
```

### Using the Package Builder online help

For detailed instructions about creating and modifying .CFG files, see the Package Builder online help. Click **Start | Programs | LANDesk Management | LANDesk Enhanced Package Builder**. Click **Help | Index** and select the following online help topics:

- Getting started with Package Builder
- Creating a simple installation
- Package Builder commands
- How does Package Builder do an installation?
- Using variables in commands and assigning values

### Modifying the registry

Commands that modify the registry begin and end with BeginRegistry and EndRegistry commands. In between these commands are the commands that



identify the registry key and the value. The Package Builder wizard flags two keys as dangerous:

- \HARDWARE
- \SYSTEM\CURRENTCONTROLSET

These keys are considered dangerous because they are usually not compatible with any computer other than the package-building computer. When these keys are modified, the Package Builder wizard places such commands within an IF `$DANGEROUS$ = "TRUE"` statement. If the changes to these keys are compatible with your target computers and you want them executed, you must define a `$DANGEROUS$` variable at the top of the script and set its value to TRUE.

# OS deployment

---

OS deployment adds automated remote image deployment capability to your managed network. OS deployment streamlines new device provisioning without requiring additional end user or IT interaction once the process starts.

---

**Note:** For information on installing the OS deployment component on your core server, and configuring your OS deployment environment, refer to the *Installation and Deployment Guide*.

---

Read this chapter to learn about:

## OS deployment

- [OS deployment overview](#)
- [OS image guidelines](#)
- [Customizing images with Setup Manager and Sysprep](#)
- [Creating imaging scripts with the OS Deployment wizard](#)
- [Modifying scripts](#)
- [PXE-based deployment](#)
- [Using PXE representatives](#)
- [Booting devices with PXE](#)
- [Configuring the PXE boot prompt](#)
- [Using LANDesk managed boot](#)
- [Using the PXE boot menu](#)
- [Using the PXE holding queue](#)
- [Scheduling OS deployment tasks](#)
- [Adding devices to the holding queue](#)

## OS deployment overview

The OS deployment (OSD) feature provides PXE-based deployment to deploy OS images to devices on your network. This allows you to image devices with empty hard drives or unusable OSes. Lightweight PXE representatives eliminate the need for a dedicated PXE server on each subnet. For more information, see [PXE-based deployment](#) later in this chapter.

If you use Microsoft's Sysprep utility to create your images, OS deployment creates customized SYSPREP.INF files and injects them into each device's image on a per device basis, customizing Windows computer names, domain information, and so on from the core database.

OS deployment includes a built-in imaging tool you can use to create images. OS deployment also supports third-party imaging tools that you may already be using, such as Symantec Ghost\* and PowerQuest DeployCenter\*.

---

**WARNING:** OS deployment (imaging) should be used with caution. Operating system deployment includes wiping all existing data from a device's hard drive and installing a new operating system. There is a substantial risk of losing critical data if the OS deployment is not performed exactly as described in this document, or if poorly implemented images are used. Before performing any OS deployment, we

recommend that you back up all data in such a manner that any lost data may be restored.

---

## OS deployment steps

When planning and implementing an OS deployment operation, follow this sequence of steps:

1. (Optional) Run the Microsoft Setup Manager and Sysprep utilities on the device whose image you want to capture.
2. Create an image capture script with the OS Deployment wizard.
3. Schedule a task with the **Scheduled tasks** tool that runs the capture image script on the device whose image you want to capture.
4. Create an image deployment script with the OS Deployment wizard.
5. Schedule a task with the **Scheduled tasks** tool that runs the deploy image script on target devices where you want the image deployed.
6. Target devices that are PXE-enabled will begin the image deployment job the next time they boot (PXE-based deployment).

Read the relevant sections below for detailed information about each of these steps.

## OS image guidelines

You can create OS images with the LANDesk imaging tool or other imaging tools. When you run the OS Deployment wizard to create an imaging script, you are prompted to specify the image type and imaging tool. The wizard automatically generates command lines for the LANDesk imaging tool, Symantec Ghost 7.5, and PowerQuest DeployCenter 5.01.1.

---

**Note:** When you install the OS deployment component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT, and BACKALL.BAT.

---

If you have a different imaging tool, you can supply the command line for it at the end of the wizard. If you specify a custom command line, the wizard will put your custom line in the right location in the script so that you don't have to edit the script manually.

## Image filenames

You should give your images unique filenames. Deploying different images with the same filename simultaneously on the same subnet can cause problems. Depending on how an imaging utility names image files, (multi-file Ghost images, for example), you may only have five unique characters in your filename once it is converted to a DOS 8.3 name format.

OS deployment creates image names using the first eight characters of the Windows computer name on which the image was created. If your image spans multiple image files, the imaging tool may only use the first five characters. When capturing images

from multiple devices, you have two ways of ensuring that your images have unique names:

- Image one device at a time, renaming each image as it's created.
- Before running the job, ensure that the first eight characters (or five characters with multi-file images) of your image Windows computer names are unique.

## Image file specifications and requirements

Regardless of the imaging tool you use, the compressed image size cannot exceed 2 GB because of DOS and disk imaging tool limitations.

OS deployment supports NTFS, FAT, and FAT32 file systems.

## LANDesk agents and images

You should not include the LANDesk agents in your images. If you use a Sysprep image, OS deployment will install the LANDesk agents after the image is restored.

If your non-Sysprep images include LANDesk agents, you will need to delete the LDISCAN.CFG file from the root of the hard drive before imaging. You will also need to delete these keys:

- HKLM\Software\Intel\LANDesk\Common API\Unique ID
- HKLM\Software\LANDesk\Common API\Unique ID

If you leave these in the image, all devices using the image will have the same core database entry. Alternatively, if you have non-Sysprep images that already have LANDesk agents on them, you can enable the **Reject duplicate identities** option on the **Duplicate device ID** dialog (**Configure** | **Services** | **Inventory** | **Duplicate ID**).

## Partitions and images

By default, when OS deployment restores an image on a target device, it deletes any preexisting partitions on that device.

The LANDesk imaging tool supports single-partition and multiple partition images (up to four partitions).

## Non-Windows images

You can use OS deployment to deploy almost any image your imaging tool supports, not just Windows-based images. When deploying non-Windows or non-Sysprep images, make sure you do not select the **Image is Sysprepped** option on the **Configure imaging task** page of the OS Deployment wizard.

## Linux image specifications and requirements

The following is a list of constraints imposed on Linux installations.

1. The root ('/') partition must be of filesystem type ext2, ext3, or xfs.
2. The root partition CANNOT be contained in an LVM PV (Logical Volume Manager - Physical Volume), but MUST be a partition (physical, or extended) in the drive's MBR (Master Boot Record).
3. The last partition is the only partition that can be expanded; therefore it, too, must be of filesystem type ext2, ext3, or xfs.
4. You must specify in the configuration wizard which drive type (IDE or SCSI) the image is to be read from or written to.
5. You must specify which partition the root partition is on (i.e., hda3 or sda2)

## Customizing images with Setup Manager and Sysprep

You can use Microsoft's Setup Manager and Sysprep utilities when deploying Windows 2000 and Windows XP images. Sysprep customizes a Windows installation so that when the OS reboots, it looks for an answer file (SYSPREP.INF) and reconfigures itself for the new device. Setup Manager creates the SYSPREP.INF answer file that Sysprep uses.

Before creating OS deployment scripts, you should run Microsoft's Setup Manager (SETUPMGR.EXE) and create a SYSPREP.INF answer file for the images you're deploying. You can then use this file as the basis for any OS deployment scripts you create by selecting the **Use existing SYSPREP.INF file as a template** option on the **Specify Sysprep file information** page of the wizard. Any OS deployment script settings you make in the wizard override the equivalent options in the template SYSPREP.INF file.

Using Sysprep on your Windows 2000/XP images allows OS deployment to query the core database for each device you're deploying and to migrate certain user settings, such as:

- Windows computer name
- Management Suite GUID (the unique identifier Management Suite uses to identify devices in the core database)

You can also set these options globally for images you deploy:

- Time zone
- Volume license key
- Registered name and organization
- Workgroup/Domain/LDAP Organizational Unit (OU)

OS deployment uses information from the core database and from the image deployment script to create a custom SYSPREP.INF for each device you're imaging. OS deployment then injects that SYSPREP.INF into each device's image.

## Creating a Sysprep image

### To create an image that uses Sysprep

1. On the device whose image you want to capture, make configuration or customization changes to prepare it for imaging.
2. At the root of the device's hard drive, make a c:\sysprep folder.
3. From a Windows 2000 or Windows XP installation CD, open \Support\Tools\DEPLOY.CAB and copy **SYSPREP.EXE** and **SETUPCL.EXE** to the sysprep folder you created.
4. Open a DOS command prompt and change to the sysprep folder. Run Sysprep. If you don't use the reboot option, you'll need to shut down the device from the Start menu once a message appears requesting that you shut down.
5. Boot to DOS and run your imaging tool manually.

### For more information on Setup Manager and Sysprep

Refer to Microsoft's Web site for official documentation about the Setup Manager and Sysprep utilities. Sysprep has many powerful features you can use that are beyond the scope of this document.

## Creating imaging scripts with the OS Deployment wizard

OS deployment provides the OS Deployment wizard that lets you create imaging (image capture and image deploy) scripts. All LANDesk Server Manager scripts are managed with the Scripts tool.

For page-by-page descriptions of the wizard's interface, see Help for the OS Deployment wizard.

With the wizard you can create scripts that perform the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device. Images can be captured using the built-in LANDesk imaging tool that installs with Server Manager, or a third-party tool such as Ghost, PowerQuest, or another tool of your choice.
- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.
- **Build a script to run DOS tasks on managed device:** Creates a script that runs DOS commands (including application launches) on devices.

Once you have created a script, you can schedule it to run on devices by using the **Scheduled tasks** tool.

If you are deploying an image to PXE-enabled devices, you can add image deployment scripts to the PXE DOS boot menu. This menu is DOS-based and appears on the device during a PXE boot. For more information, see "[Using the PXE DOS menu](#)" later in this chapter.

### To run the OS Deployment wizard

1. In the left navigation pane, click **OS deployment**.
2. Click **New** to open the wizard.
3. Select the type of script you want to create. For online help about options on any page of the wizard, click **Help**.
4. Advance through the wizard until you reach the last page. Click **Save** to save the script and exit the wizard. Once complete, the script appears in the OS deployment scripts section or in the **All OSD Scripts** group in the **Scripts** window.

Administrators (users with the LANDesk Administrator right) can copy scripts to user subgroups in the Users Scripts group.

### Additional notes on scripts

- Script names need to follow Windows file naming conventions. The wizard uses the script name you enter as the filename. If you use characters that aren't allowed in Windows filenames, you'll get an error about using invalid characters.
- All scripts are stored on the core server, in the \\<core>\LDMain\Scripts directory.
- The wizard restores the settings on each page from the last script you created. If you change the script type from an imaging task to a DOS task, the wizard clears the remembered settings.

### About DOS tasks scripts

- These remote commands are sent one line at a time.
- DOS scripts run from the virtual boot partition and go through the same network detection process as normal OS distributions do.
- The "Abort this job if any command fails" option stops execution if one of the commands returns a non-zero DOS errorlevel code. You can view DOS task status in the Custom Job window or with a report.
- For more information about script commands, see "Using Custom Scripts," a whitepaper located at <http://www.landesk.com/support/downloads>.

## Modifying scripts

You can modify your scripts at any time by using the Scripts tool or by modifying the script directly in its .INI file and modifying any existing Sysprep settings in its associated .INF file.

---

**Note:** With DOS scripts, the only changes you should make are between the REMPINGx=DOS and REMEXECx=reboot.com lines. The other lines in the script manage the virtual boot partition files and boot process.

---

### To modify a script via an .INI file

1. Navigate to the \\<core>\LDMain\Scripts directory.
2. Open the script in a text editor such as Notepad. If this script has Sysprep settings associated with it, the SYSPREP.INF file also opens in Notepad.
3. Make your changes

4. Save the file(s).

---

#### Where .INI and .INF files are saved

.INI files are saved to the \\<core>\LDMain\Scripts directory. .INF files are saved to the \\<core>\LDMain\LANDesk\Files directory.

---

#### To modify a script to work with Linux

1. Build a standard OS Deployment deploy script using the OSD deployment Wizard.
  1. Deselect **SysPrep**
  2. Set the deploy to use Ghost
  3. Modify the ghost '-clone' command-line option to include ',SZEL'. For example,

```
-clone,mode=load,src=i:\mylinux.gho,dst=1,SZEL
```

---

**Note:** There are no spaces from "-clone" through "SZEL"

---

2. Remove all lines relating to SysPrep, hal, and profiles. If you used the wizard to create the script, these lines will not exist.

```
UseExtngSysPrep=...
ExistingSysPrepFile=...
SysPrepFile=...
RemoteSysPrepCopyPath=...
IsSysPrepImage=...
RemoteProcessorPath=...
ProfileMigration=...
ProfileMigrationDomain=...
ProfileMigrationUsername=...
ProfileMigrationPassword=...
ProfileMigrationUNC=...
ProfileMigrationDefaultUserPass=...
ProfileMigrationDDF=...
ProfileMigrationForceCredentials=...
```

3. Change the fworkcl.exe line (around REMEXEC31) to use the root partitions partition number, and change the filename to be /etc/ldiscn.conf ... but with DOS-style delimiters. For example,

```
REMEEXEC31=r:\dos\fworkcl.exe /c r:\guid.pds 0 3 \etc\ldiscn.conf
```

4. Once PWORKCL.EXE is fixed insert a line between the FWORKCL.EXE and the REBOOT lines (renumber the REMEXEC's) that reads like the following (replace the last digit with your last partition number).

```
REMEEXEC33=r:\dos\pworkcl.exe /R 0 3
```



## Viewing image status reports

The device being imaged sends status updates to the core server. You can track status in the Custom Job window or with a report. As OS deployment sends imaging commands to devices, the commands appear in the Custom Job window. Devices being imaged send status updates for each script command that is sent. If image deployment fails for some reason, you can see the command that failed.

Common reasons why imaging fails include:

- Partition corruption
- Problems the imaging tool can't handle
- Network adapter auto-detection can't find a network adapter
- Undetectable network adapter you specified doesn't work. (If the network adapter driver you specify fails to load, that device will be stuck at the DOS prompt. You'll have to manually reboot it.)

OS deployment creates a status report for each job, showing if it failed or succeeded on targeted devices.

To view a status report

1. In the left navigation pane, click Reports | All LDMS reports.
2. Select the OS deployment success rate report.
3. From the list of log files, select the file for the job you're interested in viewing.
4. Click Run.

At the top of each report will be any jobs that failed on individual devices. Reports also show the details of each job, such as:

- Machine Name: For devices already scanned into the core database, this name will be the device name assigned to the device. For PXE-booted devices that haven't been inventory scanned, the machine name will be a MAC address. You can use a .CSV file to import MAC addresses into the core database. For more information, see ["Using CSVIMPORT.EXE to import inventory data."](#)
- Status: Job status, either failed or OK.
- Duration: The amount of time each command took to complete.
- Commands: Each command that ran as part of the script. If a job failed, this column shows which command caused the failure.

## PXE-based deployment

OS deployment supports PXE booting and image deployment. PXE-based deployment provides another method (in addition to agent-based deployment) of automated remote imaging of devices on your network. With PXE support, you can boot both new and existing PXE-enabled devices and either execute an OS deployment script at the device from a custom PXE DOS boot menu, or scan devices into your core database and then schedule an image deployment job with the **Scheduled tasks** tool.

PXE-based deployment is a quick and easy way to image devices in a variety of situations. For example:

- Initial provisioning of new devices
- Imaging devices in a test or training lab
- Re-imaging corrupted devices

This product offers several options for using PXE to deploy OS images. For more information, see "[Understanding the PXE boot options](#)" later in this chapter.

## PXE protocol basics

PXE (Preboot Execution Environment) is an industry-standard networking protocol that enables devices to be booted and imaged from the network, by downloading and installing an executable image file from an image server, before the device boots from the local hard drive. On a PXE-enabled device, the PXE protocol is loaded from either the network adapter's flash memory or ROM, or from the system BIOS.

PXE uses the following communication standards: DHCP (Dynamic Host Configuration Protocol), TFTP (Trivial File Transfer Protocol), and MTFTP (Multicast Trivial File Transfer Protocol).

When a PXE-enabled device boots up, it sends out a DHCP discovery request. If a DHCP server implementing PXE is found, the server assigns an IP address to the device and sends information about available PXE boot servers. After completing the DHCP discovery process, the device contacts the PXE server and downloads an image file through TFTP. The imaging script is then executed, loading the OS image from the imaging server onto the device. With Server Manager, the image file is referenced by an OS deployment script.

## Using PXE representatives

PXE support software is installed on your core server as part of the normal OSD installation. However, to enable PXE support, you must first deploy a PXE representative on each subnet of your network where you want PXE support available. PXE representatives provide scalability on your network by deploying OS images to devices in their respective subnets.

Devices on each subnet use normal PXE query and file transfer methods to communicate with their resident PXE representative, which communicates with the core server using Web services (HTTP).

---

### Disable other PXE servers

If there is *any* other PXE server currently running on your network, you must first disable it in order to use LANDesk PXE support.

---

## Deploying PXE representatives

You need to deploy at least one PXE representative on each subnet where you want to provide PXE boot support. You set up a PXE representative by running the PXE Representative Deployment script on the selected device. This predefined script is available in the **Scripts** page under the All other scripts folder.

You must create a file named ALLOWED.TXT that contains a list of MAC addresses of the machines you want the PXE Representative (Proxy) to manage. Place this file in the root directory of the PXE Representative computer.

---

**Note:** the MAC addresses should be formatted with no spaces or dashes and exist on the same subnet that the PXE Representative is located.

---

You can have multiple PXE representatives on a subnet to help with load-balancing. When this is the case, the first PXE representative to respond to a device's request is the one that will be used to communicate with the core server.

---

**Note:** We recommend that you do *not* deploy a PXE representative on your core server.

---

There are no special hardware requirements for the device you select to be a PXE representative, but it must meet the following software requirements:

- **Operating system:** Windows 2003, Windows 2000, or Windows XP.

For Windows 2003 and 2000, ensure that the Microsoft MSI service is running (XP includes MSI by default). If you have installed the latest service pack for either OS, MSI service should be running. Otherwise, you can deploy it to the target PXE representative from the console by following these steps: in the left navigation pane, click **Scripts**, then click **All other scripts**, select the **MSI service deployment** task, click **Schedule**, edit the task to target the PXE representative and schedule the task.

- **Installed LANDesk agents:** Software Distribution agent and Inventory Scanner agent. For information about installing agents, see the *Installation and Deployment Guide*.

### To deploy a PXE representative

1. In the left navigation pane, click **Scripts**. Click **All other scripts**.
2. Select the **PXE Representative Deployment** script from the list, and from its shortcut menu, click **Schedule**. Type a name for the task, and click **OK**.
3. In the **My devices** list, select the device(s) on which you want to install PXE services (in this case the core server) and click **Target**.
4. In the bottom pane, click **All tasks**, and select the task you named in step 2. Click **Edit**.
5. Finish configuring the task.

---

### Updating PXE representatives

If you modify the PXE boot option settings (in **Start | All Programs | LANDesk | LANDesk Configure Services**), you need to update all of your PXE representatives by re-running the PXE Representative Deployment script to propagate those changes to PXE representatives on each subnet. However, re-running the script is not necessary if you simply move PXE proxies from the Available proxies list to the Holding queue proxies list. For more information about the PXE holding queue, see ["Using the PXE holding queue"](#) later in this chapter.

---

### To update or remove a PXE representative

1. In the left navigation pane, click **Scripts**. Click **All other scripts**.
2. To update a PXE proxy, select the **PXE Representative Deployment** script from the list, then click **OK**. Or, to remove a PXE proxy, select the **PXE Representative Removal** script, then click **OK**.
3. In the **My devices** list, select the device(s) on which you want to install PXE services (in this case the core server) and click **Target**.
4. In the bottom pane, click **All tasks**, and select the task you named in step 2. Click **Edit**.
5. Finish configuring the task.

## Booting devices with PXE

When a PXE-enabled device boots, the following occurs:

1. The PXE-enabled device sends out a query for PXE services running on a PXE representative on the network.
2. If a PXE representative exists on the subnet, it responds and tells the device to continue to boot using PXE.
3. A PXE boot session is initiated on the device and the PXE boot prompt displays. The default prompt message displays for four seconds and says "Press F8 to view menu." (You can modify these PXE boot prompt settings in **Start | All Programs | LANDesk | LANDesk Configure Services**.)
4. If the **F8** key is pressed before the countdown expires, a preliminary PXE boot menu appears, allowing you to choose from the following boot options:
  - **Local boot:** The device boots to the local hard drive. If no OS is present, an error message appears.
  - **LANDesk Managed Boot:** The device is added to the console's **My devices** page (displays the device's MAC address), where you can schedule an OS deployment script to run on it.
  - **LANDesk Boot Menu:** The device displays the boot menu you created with the PXE Boot Menu tool, and you can select an OS deployment script to run on it. For more information, see [Using the PXE Boot Menu](#) later in this chapter.
5. If you don't press the **F8** key before the countdown expires, the device will use the default boot option. The default boot option is determined by the following conditions:
  - If the device detects a scheduled imaging job for itself in the core database (either a failed or pending job), the default boot option becomes **LANDesk managed boot**.
  - If the device does *not* detect an image job for itself, the default boot option becomes **Local boot**.
  - The **PXE DOS menu** will never become the default boot option.
6. The scheduled OS deployment script runs on the device.

## Understanding the PXE boot options

This section provides information on configuring the PXE boot prompt, and how to use the following PXE boot options:

- LANDesk managed boot
- PXE Boot menu
- PXE holding queue

### Configuring the PXE boot prompt

You can control how the PXE boot prompt behaves when devices attempt to PXE boot.

When a PXE-enabled device boots up, a DHCP request attempts to initiate a PXE session by looking for a server (or PXE Representative) running PXE services software (PXE and MTFTP services). If the device discovers a PXE server, the PXE boot prompt displays on the device for a specified number of seconds. By pressing the F8 function key during this countdown, you access the PXE boot menu and can select an OS image to deploy on the device.

---

**Note:** If you have PXE representatives running on subnets of your network, and you want to implement PXE boot prompt changes to any of those proxies, you must run or re-run the PXE Representative Deployment script on the proxy.

---

#### To configure PXE boot prompt options

1. In the Start menu, click **Programs | LANDesk | LANDesk Configure Services**, then click the **OS deployment** tab.
2. Enter a value (in seconds) in the Timeout option. The default value is 4 seconds. The maximum number of seconds you can enter is 60 seconds.
3. Type a message in the Message text box. The default message is "Press F8 to view menu." The maximum number of characters you can type is 75 characters.
4. Click **Apply** to save your changes, or click **OK** to save your changes and close the dialog.

#### To implement PXE boot prompt changes to a PXE representative

1. In the left navigation pane, click **Scripts**. Click **All other scripts**.
2. Select the **PXE Representative Deployment** script from the list, then click **OK**.
3. In the **My devices** list, select the device(s) on which you want to install PXE services (in this case the core server) and click **Target**.
4. Select the **PXE representative deployment** script, and from the task's shortcut menu, click **Edit** and finish configuring the task.

## Using LANDesk managed boot

LANDesk managed boot is the default boot option when a PXE-enabled device boots and detects a failed image deployment script or failed DOS task script for it in the core database. You can also select this boot option manually at the device when the boot option menu appears.

Because it allows unattended deployment, LANDesk managed boot is useful for pre-targeting devices for imaging. For example, you could pre-target new devices for a particular OS image even before they arrive by importing a .CSV file containing device MAC addresses into the core database. For more information, see "[Using CSVIMPORT.EXE to import inventory data.](#)"

### To pre-target devices with the LANDesk managed boot option

1. Before the PXE-enabled devices are connected to the network, add their identifications to the core database by importing a .CSV file.
2. Schedule an image deployment job for the devices.
3. The imaging job fails because the devices are not yet connected to the network.
4. Connect the devices to your network and boot them.
5. The devices detect a failed imaging job and default to the LANDesk managed boot option.
6. The previous failed image deployment job automatically launches and images the target devices.

## Using the PXE boot menu

The PXE boot menu lets you interactively select an image deployment script for a device without having to schedule an image deployment job. This method might be useful when you have to re-image corrupted devices. Before using the PXE boot menu, you must first configure it by adding the OS deployment scripts you want to display in the menu.

You build the PXE boot menu system by creating directories and placing pre-configured OS deployment scripts in those directories. The script's description appears as a menu item in the PXE boot menu on the device.

### To configure the PXE boot menu

1. In the bottom pane of the **OS deployment** window, click the **PXE boot menu** tab.
2. To add a new directory or subdirectory to the menu system, click the **New folder** toolbar button.

**Note:** Subdirectories can extend four levels from the top directory.

3. Type a name for the directory. For example, the directory name could describe the OS platform or version number of the images contained in that directory. You can also change the name of the directory at any time by clicking the **Rename** toolbar button (or right-clicking the directory and selecting **Rename**).

4. In the top pane, select scripts you want to move to the appropriate directory in the PXE Boot Menu window. In the bottom left pane, select the folder you want to move the scripts to, and click **Add selected scripts**.

**Note:** A maximum of 18 scripts can be placed in each directory.

5. To save the PXE boot menu and update the PXE Representative with a modified menu, click the **Update** toolbar button. (Note that you must click the **Update** button here in the console if you want changes to appear in the PXE boot menu on PXE devices when they boot.)

### To access the PXE boot menu from a device

1. Boot a PXE-enabled device.
2. When the PXE boot prompt displays, press the **F8** key before the countdown expires. Select **LANDesk(R) PXEBoot menu**. The menu system that you configured in the console's PXE Boot Menu window appears.
3. To open a directory and view its subdirectories and images, type the number of the directory and press **Enter**. Navigate the menu system and find the image you want deployed on the device. You can press **B** to go back one level, or press **X** to exit the menu system.

**Note:** If you exit the menu system without making a selection, the device will wait for a scheduled imaging job from Server Manager.

4. To select an OS image (referenced in an OS deployment script), type the number of the script and press **Enter**. The script runs and the image is loaded on the device.

## Using the PXE holding queue

The PXE holding queue is another method for remotely deploying OS images to PXE-enabled devices. This method is especially useful in these situations:

- In a controlled lab environment where you frequently need all devices re-imaged with an identical image.
- For imaging "bare-metal" devices in a lab that can then be moved into their appropriate production environment.

Devices can then be scheduled for an image deployment job. This product does not support agent-based deployment. You can schedule devices after they are in the holding queue.

### To configure a PXE holding queue

1. Set up PXE representatives on your network.
2. In the Start menu, click **Programs | LANDesk | LANDesk Configure Services**, then click the **OS deployment** tab.
3. Select and move PXE representatives from the Available proxies list to the Holding queue proxies list.

The Available proxies list shows all available PXE representatives on your network, identified by device name. This list is generated by running an inventory scan that detects PXE software (PXE and MTFTP protocols) running on the device. The inventory scan is run automatically whenever a PXE representative is initially set up.

4. Click **Reset**. The Reset button forces all PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the PXE holding queue in the console's network view. These devices can then be scheduled for an imaging job.

**Note:** The Reset button is enabled when you select a PXE representative in the Holding queue proxies list.

5. Click **Apply**, then **OK** to save your changes and close the dialog.

The next time a device on that subnet boots, it will be added to the PXE holding queue object in the console's network view.

#### To deploy an image to a device in the PXE holding queue

1. In the **Holding queue** tab, click a device and click an OS deployment script, then click **Schedule task**.

---

**NOTE:** The device will be removed from the Holding Queue once the device has been assigned (targeted) to an OS Deployment task.

---

### To schedule an OS deployment task

1. In the left navigation pane, click **OS deployment**.
2. In the bottom pane, click **Holding queue**.
3. Click **Schedule task**.
4. Fill out the pages of the custom script task. Click the Help button for help on any page, or see the [Task scheduler](#) help.

When you click **Schedule task**, a task is created (it has no targeted devices, and it is unscheduled). If you cancel this Scheduled task procedure, please be aware that it has still been created and appears in the Task list.

### To add devices to the holding queue

Use the New MAC address dialog to add devices to the OS deployment holding queue so they can have operating systems deployed to them. This is particularly helpful for the initial provisioning of new devices.

#### To enter a new device

1. In the left navigation pane, click **OS deployment**.
2. In the bottom pane, click **Holding queue**.
3. Click **Add devices**.



4. Type the MAC address (without dashes or colons) in the **MAC address box**. If the machine's vendor didn't provide you with the MAC address, NIC vendors often provide utilities to find the MAC address. If the machine already has an OS, you can find the MAC address on a Windows machine by typing "ipconfig /all" at the command prompt (look under the "Physical Address field"), or on a Linux machine type "ifconfig."

If the device has multiple NICs, be sure to enter the MAC address of the NIC you plan to use. If you enter one address and OSD uses another, the deployment will not work.

5. Type the display name in the **Display name box**. While the display name is optional, it is highly recommended. On a bare-metal device, the Display name is the only differentiator in the OS deployment view.
6. Type the OS type in the **OS type box**.
7. When you are done, click **Add** to add the device to the New MAC address table.
8. To import a device or list of devices, type the location of a text file (CSV) which contains MAC address information in the text box (or click **Browse** to find the file) and click **Import**.

The imported addresses in the CSV file must be in the following format: <MAC address>, computername, OSname

9. Click **Save** to save the contents of the New MAC address table to the database.

# Scheduling tasks

---

## Scheduling tasks

- [Target devices page](#)
- [Schedule task page](#)
- [Credentials page](#)
- [Image Information page](#)
- [Additional commands page](#)
- [LANDesk agent page](#)
- [DOS commands page](#)
- [Custom scripts page](#)

The Scheduled tasks tool is common to Configure agents, Scan vulnerabilities, Distribute software, Discovery, Scripts, and OS deployment. The tasks are filtered in the lower pane of the specific feature pages to show only related tasks. For example, if you open the Discover devices tool, discovery tasks are displayed in the Discovery tasks tab in the lower pane of the Discover devices page. All tasks are still visible through the Scheduled tasks tool. Here you can schedule configurations to run immediately, at some point in the future, on a recurring schedule, or run just once.

The left pane of the Scheduled tasks page shows these task groups:

- **My tasks:** Tasks that you have scheduled. Only you and administrative users can see these tasks.
- **All tasks:** Both your tasks and tasks marked public.
- **Common tasks:** Tasks that users have marked common. Anyone who schedules a task from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group for that user.
- **User tasks** (administrative users only): Tasks users have created.

When you click My tasks, Common tasks, or All tasks, the right pane shows this information:

- **Task:** The task names.
- **Start On:** When the task is scheduled to run. Click a task name and click **Edit** to edit the start time or to reschedule it.
- **Status:** The overall task status. View the right pane Status column for more details. The right pane column shows the task status, which can be Working, All Completed, None Completed, or Failed.
- **Distribution package:** The package name the task distributes.
- **Delivery method:** The delivery method the task uses.
- **Owner:** The name of the person who originally created the script this task is using.

When you double-click a scheduled task, the right pane shows this summary information:

- **Name:** The task state name.
- **Quantity:** The number of devices in each task state.
- **Percentage:** The percentage of devices in each task state.

Before you can schedule tasks for a device, it must have the appropriate agent and be in the inventory database. Server configurations are an exception. They can target a device that doesn't have the standard LANDesk agent. Tasks can be rescheduled (edited) or deleted from the Tasks tabs. Once you schedule a task, see the Tasks tab for task status.

You can edit a task by selecting the task you want to edit and clicking **Edit**. The task opens with editing options applicable to the task.

### About the Target devices page

Use this page to add device targets for the task you're configuring. You can also see the targeted devices, queries, and device groups for the task on this tab. Device groups are created in Management Suite, and are viewable in Server Manager. This page is not needed for Discovery tasks.

- **Add target list:** Add the devices previously put in the target list from My devices.
- **Add query:** Targets the results of a query that you've previously created.
- **Remove:** Removes the selected targets.

### About the Schedule task page

The Scheduler contains a Scheduled task – properties tab that includes these options.

- **Leave unscheduled:** (default) Leaves the task in the Task list for future scheduling.
- **Start now:** Runs the task as soon as possible. It may take up to a minute for the task to start.
- **Start later:** Starts the task at the time you specify. If you click this option, you must enter the following:
  - **Time:** The time you want the task to start
  - **Date:** The date you want the task to start. Depending on your locale, the date order will be day-month-year or month-day-year.
  - **Repeat every:** If you want the task to repeat, click whether you want it to repeat **Daily**, **Weekly**, or **Monthly**. If you pick **Monthly** and the date doesn't exist in all months (for example, 31), the task will only run in months that have that date.
- **Schedule these devices:** For the first time a task runs, you should leave the default of Waiting or currently working. For subsequent runs, choose from All, Devices that didn't succeed, or Devices that didn't try to run the task. These options are explained in more detail below.
  - **All:** Select this if you want the task to run on all devices, regardless of state. Consider using this option if you have a task, especially a repeating one, that needs to run on as many devices as possible.
  - **Devices that didn't succeed:** Select this if you only want the task to run on all devices that didn't complete the task the first time. This excludes devices that have a Successful state. The task will run on devices in all other states, including Waiting or Active. Consider using this option if you need the task to run on as many unsuccessful devices as possible, but you only need the task to complete successfully once per device.
  - **Devices that didn't try to run the task:** Select this if you only want the task to run on devices that didn't complete the task and didn't fail the task. This excludes devices that were in an Off, Busy, Failed, or Canceled state. Consider using this

option if there were a lot of target devices that failed the task that aren't important as targets.

### About the Credentials page

- **Username:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password:** Provides the user's password.
- **Domain:** Provides the user's Active Directory domain.

### About the Image information page

Use this page to specify the type of image you want to restore with this script, where the image is stored, and where the imaging tool is located:

- **Image type:** Identifies the file type (format) of the existing image file you want to deploy with this script, selected from the list of imaging tools.
- **UNC path to image file to restore:** Locates the server and share where the image file is stored, including the image filename. The image must be stored on a share accessible to devices.
- **UNC path to imaging tool:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename.

### About the Additional commands page

- **Enter commands to run before the device is rebooted and imaged:** Enter commands to be executed prior to the device being rebooted and imaged.
- **Enter additional command line parameters for the imaging tool:** Enter any additional parameters not previously specified.

### About the LANDesk Agent page

- **UNC path:** The path to the agent package.
- **Username:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password:** Provides the user's password.
- **Domain:** Provides the user's Active Directory domain.

### About the DOS commands page

- **DOS commands:** Enter DOS commands you want to be executed on the device at the time of the deployment.
- **Abort this job if any command fails:** Stops the task should any command fail to execute and restores the device to its previous state.

### About the Custom scripts page

- **Currently selected custom script:** Select the script you want to schedule.



# Reports

---

## About reports

Server Manager includes a reporting tool you can use to generate a wide variety of specialized reports that provide critical information about the managed devices on your network.

Server Manager uses an inventory scanning utility to add devices (and collected hardware and software data about those devices) to the core database. You can view and print this inventory data from a device's inventory view, as well as use it to define queries and group devices together. The reporting tool takes further advantage of this scanned inventory data by collecting and organizing that data in useful report formats.

You can use the predefined Server Manager service reports and inventory asset reports. After running a report, you can view it from the Server Manager console.

If you have Server Manager and System Manager installed together, the reports you run in Server Manager will only include servers. If you run a query you will get both servers and other devices, unless the query has been configured to exclude other devices.

## Understanding report groups and predefined reports

Reports are organized in groups in the **Reports** window (left navigation pane | **Reports**). Administrators can view the contents of all of the report groups. Server Manager includes a specific role, called Reporting, to allow others to view Server Manager reports without providing them access to other management capabilities. (For more information, see [Role-based administration](#).) Users with the Reporting right can also see and run reports, but only on the devices included in their scope.

The **Reports** window has the following groups of reports:

- Hardware
- Software
- Other

## Viewing reports

You can run any report from the **Reports** window.

From the **Reports** window, click a report group, then click the report you want to run. The report data displays in the **Report view**.

## About the Report view window

Reports allow you to quickly access a graphical representation of the assets on your client computers. The reports are created from data the scanner stores in the database. You can view reports or print them through your browser.

### To view a report

1. In the left navigation pane, click **Reports**. Report categories are listed in the right pane. Click a category heading to view the list of reports. An icon next to each report indicates the report type.



A report with a chart icon next to it displays as a pie or bar chart (two- or three-dimensional). In a chart, you can click on any colored bar or pie section to drill down to a summary.



A report with a document icon next to it displays as text.

2. Click the report name to view the report.
3. For the hardware or software scan date summaries, click the start and end dates to set the time frame, then click **Run**.

The Disk Space Summary report contains data for Windows-based servers only.

To print a report, right-click the page and click **Print**. On the Print dialog, click **Print**. If a report spans multiple pages, you must right-click in each page to print it.

### To distribute a report

- To e-mail a report, the recommended method is to print the report to a .PDF file, then attach it to the e-mail.

---

The console displays report charts as pie or bar charts. To set the chart type, click the drop-down list in the report chart, then change the chart type.

In order to view the interactive bar and pie charts displayed in many reports, you must have Macromedia Flash Player\* 7 installed.

---

# Queries

---

## Using queries

Queries are customized searches of your core databases. Server Manager provides tools that let you create *database queries* for devices in your core database, as well as a method for you to create *LDAP queries* for devices located in other directories. You create core database queries in the console's **Query** view. Server Manager public queries are visible in LANDesk Management Suite, and vice-versa, if both are being used. You create LDAP queries with the **Directory manager** tool.

Read this section to learn about:

- [Queries overview](#)
- [Query groups](#)
- [Creating database queries](#)
- [Running queries](#)
- [Importing and exporting queries](#)

## Queries overview

Queries help you manage your network by allowing you to search for and organize devices in the core database based on specific system or user criteria.

For example, you can create and run a query that captures only devices with a processor clock speed of less than 166 MHz, or with less than 64 MB of RAM, or with a hard drive of less than 2 GB. Create one or more query statements that represent those conditions and relate statements to each other using standard logical operators. When the queries are run, you can print the results of the query, and access and manage the matching devices.

If you have Server Manager and System Manager installed together, the reports you run in Server Manager will only include servers. If you run a query you will get both servers and other devices, unless the query has been configured to exclude devices.

## Query groups

Queries can be associated with groups in the **My devices** view. These are called dynamic groups, and the contents of a dynamic group are the result of the query associated with that dynamic group. For example, a group comprising all the devices in a geographic area can be associated with a query on memory, hard disk size, and so forth.

For more information on how query groups and queries display in the **All devices** view, and what you can do with them, see [Grouping devices for actions](#).

## Creating database queries

Use the **New query** dialog to build a query by selecting from attributes, relational operators, and attribute values. Build a query statement by choosing an inventory



attribute and relating it to an acceptable value. Logically relate the query statements to each other to ensure they're evaluated as a group before relating them to other statements or groups.

### To create a database query

1. In the console's **Queries** view, click **New**.
2. Select a component from the inventory attributes list.
3. Under **Step 1: Search conditions**, click **Edit**.
  1. Drill down this list to select the attributes that will be your search condition. For example, to locate all clients running a particular type of software, you would select Computer.Software.Package.Name.
  2. After selecting the attributes, you'll notice that a series of fields appear in the right side of the window. From these fields, select an operator and value to complete the search condition. For example, to locate all clients running Internet Explorer 5.0, the attributes would be "Computer.Software.Package.Name," the operator "=", and the value "Internet Explorer 5."
  3. At the bottom of the window, click **Add** to fill in the empty field with your search condition.
  4. You can continue to refine the query by creating another search condition, then adding it to the first with a boolean operator (AND or OR). Also use the buttons to add, delete, replace, group, or ungroup the conditions you create.
  5. When you're finished, click **OK**.
4. Under **Step 2: Attributes to display**, click **Edit**.
  1. Drill down this list to select an attribute to display in the query results list. Remember to select attributes that will help you identify the clients returned in the query. If you cannot find attributes you want to display, you can add them in the [Custom attributes](#) dialog. However, these attributes must be assigned to machines before they appear in the query dialog.  
**Note:** If you're using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, and so on).
  2. After you've selected an attribute, click >> to move it into the empty field on the right side of the window. If you want to enumerate your query results list, click **Include count**.
  3. Repeat the process if you want to add more attributes. Use the arrow buttons to add or remove attributes, and click **Move up/Move down** to change the order of attributes.
  4. Click **Make results targetable** to enable the results of the query to be targetable for any actions you specify.
  5. When you're finished, click **OK**.
5. (optional) Under **Step 3: Sort results by attribute**, click **Edit** to customize the order of query results.
6. If you want to run the query additional times, click **Save query**, and enter a unique name for the query. If you run the query prior to saving it, the query parameters are lost and must be reconstructed to run the same query again.
7. Under **Step 4: Run query**, click **Run query**.

## About the New query dialog

Use this dialog to create a new query with the following functions:

- **Name:** Identifies the query in query groups.
- **Machine components:** Lists inventory components and attributes the query can scan for.
- **Relational operators:** Lists relational operators. These operators determine which description values for a certain component will satisfy the query.

The Like operator is a new relational operator. If a user doesn't specify any wild cards (\*) in their query, the Like operator adds wildcards to both ends of the string. Here are three examples of using the Like operator:

Computer.Display Name LIKE "My Machine" queries for: Computer.Display Name LIKE "%AI's Machine%"

Computer.Display Name LIKE "AI's Machine\*" queries for: Computer.Display Name LIKE "AI's Machine%"

Computer.Display Name LIKE "\*AI's Machine" queries for: Computer.Display Name LIKE "%AI's Machine"

- **Display scanned values:** Lists acceptable values for the chosen inventory attribute. You can also manually enter an appropriate value, or edit a selected value, with the **Edit values** field. If the selected relational operator is Exists or Does Not Exist, no description values are possible.
- **Logical operator:** Determines how query statements logically relate to each other:
  - **AND:** Both the previous query statement AND the statement to be inserted must be true to satisfy the query.
  - **OR:** Either the previous query statement OR the statement to be inserted must be true to satisfy the query.
- **Insert:** Inserts the new statement into the query list and logically relates it to the other statements according to the listed logical operator. You can't choose this button until you've built an acceptable query statement.
- **Edit:** Lets you edit the query statement. When you're finished making changes, click the **Update** button.
- **Delete:** Deletes the selected statement from the query list.
- **Clear all:** Deletes all statements from the query list.
- **Query list:** Lists each statement inserted into the query and its logical relationship to the other listed statements. Grouped statements are surrounded by parentheses.
- **Group ( ):** Groups the selected statements together so they're evaluated against each other before being evaluated against other statements.
- **Ungroup:** Ungroups the selected grouped statements.
- **Filters:** Opens the **Query filter** dialog that displays device groups. By selecting device groups, you limit the query to only those clients contained in the selected groups. If you don't select any groups, the query ignores group membership.
- **Select columns:** Lets you add and remove columns that appear in the query results list for this query. Select a component, and then click the right-arrow button to add it to the column list. You can manually edit the Alias and Sort Order text, and your changes will appear in the query results list.
- **Save:** Saves the current query. When you save a query before running it, the query is stored in the core database and remains there until you delete it.

---

**Query statements are executed in the order shown**

If no groupings are made, the query statements listed in this dialog are executed in order from the bottom up. Be sure to group related query items so they're evaluated as a group; otherwise, the results of your query may be different than you expect.

---

## Running queries

### To run a query

1. In the **All devices** view, expand the query groups to locate the query you want to run.
2. Right-click the query and select **Run query**.

Or

3. To make changes to the query before running it, double-click the query, modify steps 1-3, and then click **Run query**.

**Note:** If you have modified the query and want to save your changes, click **Save query** to save the changes or **Save query as** to give the modified query a new name. Do this before running the query. If you do not save your changes before running the query, the changes will not be saved with the query.

4. The results (matching devices) display in the right-hand pane of the **All devices** view.

## Importing and exporting queries

You can use import and export to transfer queries from one core database to another. You can import Server Manager exported queries as .XML files.

### To import a query

1. Right-click the query group where you want to place the imported query.
2. Select **Import** from the shortcut menu.
3. Navigate to the query you want to import and select it.
4. Click **Open** to add the query to the selected query group in the **All devices** view.

### To export a query

1. Right-click the query you want to export.
2. Select **Export** from the shortcut menu.
3. Navigate to the location where you want to save the query (as an .XML file).
4. Type a name for the query.
5. Click **Save** to export the query.

## Understanding custom queries

Custom queries are useful when you want inventory details about hardware and software installed on your devices. Use a custom query to build a list of computers that have similar inventory. Custom queries are also used to define groups and scopes.

The **Custom queries** page (click **Queries** in the left navigation pane) displays a list of queries that you have saved. To run a saved query, select the query, then select **Run**.

---

If the query list spans multiple pages, use the arrows at the top of the page to navigate between pages. Enter the number of items to display per page and click **Set**.

---

## Creating custom queries

Custom queries are useful when you want inventory details about hardware and software installed on your devices. Use a custom query to build a list of devices with similar inventory. For example, if you want to upgrade all devices to at least a 750 MHz processor, you can query for all devices in your database with processor speeds of less than 750 MHz. Custom queries are also used to define groups and scopes.

You can query on any of the inventory items (known as "attributes") that the inventory scanner stores in the database, as well as any custom attributes.

## Managing queries

Manage queries in the **Queries** view. Use this view to create, edit, or delete queries:

- To run an existing query, select it and click **Run**.
- To create a new query, click **New**. Once you have created and saved that query, its name will appear in the list on this page.
- To edit a query in the list, double-click it. The **Edit query** page appears with query parameters you can edit.
- To edit the most recent query, click **Edit current query**.
- To delete a query, select the query and click **Delete**.

Creating a query is a four-step process:

1. **Create a search condition:** Specify a set of inventory attributes that will be the basis of your query.
2. **Select attributes to display:** Refine or "filter" the query so that the results display the attributes most useful to you, such as IP addresses or computer device names.
3. **Sort results by attributes (optional):** Specify how you want the query results sorted. (Only applies if, in Step 2, you selected to display more than one type of attribute in the query results.)
4. **Run the query:** Run the query you just created. You can also save it for later use, or clear all of the query information to begin again.

## Step 1: Creating a search condition (required)

A search condition is a set of inventory attributes and associated values that you query for. You can use one search condition or group several together to form the basis of a query.

The following steps take place on the **Edit query** page. From the **Run queries** view, click **New**, or select an existing query and click **Edit**.

### To create a search condition

1. Under **Step 1**, click **Edit**. A window appears showing a list that represents all of the inventory data currently in the database.
2. Drill down this list to select the attributes that will be your search condition. For example, to locate all clients running a particular type of software, you would select Computer.Software.Package.Name.
3. After selecting the attributes, you'll notice that a series of fields appear in the right side of the window. From these fields, select an operator and value to complete the search condition. For example, to locate all clients running Internet Explorer 5.0, the attributes would be "Computer.Software.Package.Name," the operator "=", and the value "Internet Explorer 5."
4. At the bottom of the window, click **Add** to fill in the empty field with your search condition.
5. You can continue to refine the query by creating another search condition, then adding it to the first with a boolean operator (AND or OR). Also use the buttons to add, delete, replace, group, or ungroup the conditions you create.
6. When you're finished, click **OK**.

To run and store a query on the health status of servers (Computer.Health.State), you should be aware that the state in the database is represented by a number. Use the table below to create search conditions. For example, to create a search condition for machines with "Unknown" health, use the operator "NOT EXIST."

### Health condition Operator

Unknown	NOT EXIST
Normal	2
Warning	3
Critical	4

## Step 2: Selecting attributes to display (required)

For Step 2, select the attributes that will be most useful for identifying computers returned in the query results. For example, if you want results that help you physically locate each computer matching the search condition set in Step 1, you

would specify attributes such as each computer's display name (Computer.DisplayName) or IP address (Computer.Network.TCPIP.Address).

The following steps take place on the **Edit query** page.

#### To select attributes to display

1. Under **Step 2**, click **Edit**. A window appears showing a list that represents all of the inventory data currently in the database.
2. Drill down this list to select an attribute to display in the query results list. Remember to select attributes that will help you identify the clients returned in the query. If you cannot find attributes you want to display, you can add them in the [Custom attributes](#) dialog. However, these attributes must be assigned to machines before they appear in the query dialog.  
**Note:** If you're using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, Computer.DisplayName, Computer.Device Name, Computer.Device ID, Computer.Login Name, and so on).
3. After you've selected an attribute, click >> to move it into the empty field on the right side of the window. If you want to enumerate your query results list, click **Include count**.
4. Repeat the process if you want to add more attributes. Use the arrow buttons to add or remove attributes, and click **Move up/Move down** to change the order of attributes.
5. Click **Make results targetable** to enable the results of the query to be targetable for any actions you specify.
6. When you're finished, click **OK**.

You can also add column heading(s) to your query results list.

#### To change column headings (optional)

1. Under **Step 2**, click **Edit**.
2. In the bottom box, click a column heading and click **Edit**. Edit the heading and press **Enter**. Repeat as necessary.
3. Click **OK**.

At this point, you may want to save your query; the next procedure in the query-creation process is optional and applies only to query results that contain two or more columns. To save your query, click **Save Query** at the top of the page. A window appears prompting you to type a name for this query. Type a name, then click **Save** in the top right corner of the window.

## Step 3: Sorting results by attribute (optional)

This procedure is necessary only if you defined more than one attribute and column heading in Step 2 and now want to sort the results alphabetically or numerically within one of those columns.

For example, let's say you specified two different attributes to display in the query results: the IP address and the processor type of each returned computer. In Step 3, you could sort alphabetically by processor type in the results.

If you skip this step, the query will automatically sort by the first attribute selected in Step 2.

#### To sort results by attribute

1. Under **Step 3**, click **Edit**. A window appears showing the attributes you selected in **Step 2**.
2. Select which attribute you want to sort by, then click >> to move it over to the empty text box.
3. Click **OK**.

## Step 4: Running the query

After creating your query, you can run, save, or clear it to start over.

To save the query for future use, click the **Save** toolbar button. The query now appears in the list on the **Custom queries** page. If your query is a modified version of another, click the **Save as** toolbar button to give it a new name.

By default, saved queries are only visible by the person who saved them. If you check **Public query** before saving, the saved query will be visible to all users. Only administrators with the public query management right can make a query public.

Management Suite and Server Manager share queries. If you save a query in Management Suite, it will also be visible in Server Manager, and the reverse is true too.

To view the results of this query, click the **Run** toolbar button.

To clear the query parameters from the **Edit query** page, click the **Clear** toolbar button. If the query has already been saved, it's cleared from this page but remains in the **Custom queries** list.

## Viewing query results

Query results match the search criteria you specified in the query-building process. If the results aren't what you expected, go back to the **Edit query** page and refine the information.

To drill down to more information about one of the devices in the list of query results, double-click the query data or right-click and click **View computer** in the resulting menu.

From the **Query results** page, you can click the **Save as CSV** toolbar button to export the results into a format compatible with spreadsheet or other applications.

To print the query results, click **Print view** in the query results page.

## Viewing drill-down query results

Query results match the search criteria you specified in the query-building process. If the results aren't what you expected, go back to the **Edit query** page and refine the information.

To drill down to more information about one of the devices in the list of query results, double-click the query data or right-click and click **View computer** in the resulting menu.

## Exporting query results to CSV files

To view your query results data in a spreadsheet application, export the data as a comma-separated values (CSV) file. From the **Query results** page, click the **Save as CSV** toolbar icon to save your information as a CSV file. You can then use an application like Microsoft Excel\* to import and work with the CSV file.

## Changing query column headings

1. Open an existing query or create a new query.
2. In the bottom box, click a column heading and click **Edit**. Edit the heading and press **Enter**. Repeat as necessary.
3. Click **OK**.

## Exporting and importing queries

You can export and import any queries you create. All queries export as XML files. If you export the same query filename more than once, it will overwrite the existing file. To avoid this, you may want to copy the file to another location once it's exported.

The export and import features are useful in two scenarios:

- If you need to reinstall your database, use the export/import features to save your existing queries for use in a new database.

For example, you could export the queries, then move them to a directory unaffected by a database reinstall. After reinstalling the database, you could move the queries back into the queries directory on your Web server, then import them into the new database.

- You can use the export/import features to copy queries to other databases.

For example, you could export a query to a queries directory on your Web server, then e-mail or FTP it to someone. That person could then place the queries into the queries directory on another Web server, then import them into a different database. You could also map a drive and directly copy queries into the queries directory on another Web server.

### To export a query

Complete these steps while connected to a database that has a query you want to export.

1. In the left navigation pane, click **Queries**.
2. On the **Custom queries** page, click the query name you want to export. Click **Edit**.



3. On the **Edit query** page, click the **Export** toolbar button to export the query to disk.
4. On the **Query exported** page, right-click the query to download it as an XML file to a selected directory. The query becomes the XML file.

Note that If you export the same query filename more than once, it will overwrite the existing file. To avoid this, you may want to copy the file to another location once it's exported.

If you want to eventually import the query back into a database, you must move it to the queries directory recognized by the Web server, by default  
c:\inetpub\wwwroot\LANDesk\ldsm\queries.

### To import a query

Complete these steps while connected to a database to which you want to import a query.

1. In the left navigation pane, click **Queries**.
2. On the **Custom queries** page, click **New**.
3. On the **Edit query** page, click the **Import** toolbar button.
4. Select the query you want to import. If you want to verify the parameters of this query before importing it, click **View**.
5. Click **Import** to load the query in the **Edit query** page.
6. Once the query is loaded, scroll down and click **Save query** to save it into this database.

## LDAP queries

# Inventory management

---

## Managing inventory

You can use the inventory scanning utility to add devices to the core database and to collect devices' hardware and software data. You can view, print, and export inventory data. You can also use it to define queries, group devices together, and generate specialized reports.

Read this section to learn about:

- [Inventory scanning overview](#)
- [Viewing inventory data](#)

## Inventory scanning overview

When you configure a device with the device setup feature, the inventory scanner is one of the components that gets installed on the device. When creating a client configuration, you can specify when the inventory scanner runs on the device.

The inventory scanner runs automatically when the device is initially configured. The scanner executable is named LDISCAN32.EXE for Windows and LDISCAN for Linux. The inventory scanner collects hardware and software data and enters it into the core database. After that, the hardware scan runs each time the device is booted, but the software scan only runs at an interval you specify. To schedule a software scan, run SVCCFG.EXE in **Program Files | LANDesk | Management Suite**.

For more information on configuring the inventory service, see [Configuring the Inventory service](#) in Appendix C.

After the initial scan, the inventory scanner can be run from the console as a scheduled task. The standard LANDesk agent must be running on remote devices to schedule an inventory scan to them.

---

**Note:** A device added to the core database using the discovery feature has not yet scanned its inventory data into the core database. You must run an inventory scan on each device for full inventory data to appear for that device.

---

You can view inventory data and use it to:

- Customize the **All devices** list columns to display specific inventory attributes
- Query the core database for servers with specific inventory attributes
- Group devices together to expedite management tasks, such as software distribution
- Generate specialized reports based on inventory attributes
- Keep track of hardware and software changes on devices, and generate alerts or log file entries when such changes occur

Read the sections below to learn more about how the inventory scanner works.

## Delta scanning

After the initial full scan is run on a device, subsequent running of the inventory scanner only captures delta changes and sends them to the core database. Use the scanner option /RSS to gather software information from the Windows registry.

## Forcing a full scan

If you want to force a full scan of the device's hardware and software data, use the following method:

- Delete the INVDELTA.DAT file from the server. A copy of the latest inventory scan is stored locally as a hidden file named INVDELTA.DAT on the root of the hard drive. (The LDMS\_LOCAL\_DIR environment variable sets the location for this file.)
- Add the **/sync** option to the inventory scanner utility's command line. To edit the command line, right-click the **Inventory Scan** shortcut icon and select **Properties | Shortcut**, and then edit the **Target** path.
- On the core server, set the Do Delta registry key to 0. This key is located at: HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Do Delta

## Scan compression

Inventory scans performed by the Windows inventory scanner (LDISCAN32.EXE) are compressed by default. The scanner compresses full scans and delta scans with approximately an 8:1 compression ratio. Scans are first built completely in memory, then compressed and sent to the core server using a larger packet size. Scan compression requires fewer packets and reduces bandwidth usage.

## Scan encryption

Inventory scans are now encrypted (TCP/IP scans only). You can disable inventory scan encryption by setting the core server's Disable Encryption registry key to 0. This key is located at:  
HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Disable Encryption

# Viewing inventory data

Once a device has been scanned by the inventory scanner, you can view its system information in the console.

Device inventories are stored in the core database, and include hardware, device driver, software, memory, and environment information. You can use the inventory to help manage and configure devices, and to quickly identify system problems.

You can view inventory data in the following ways:

- [Summary inventory](#)
- [Full inventory](#)
- [Viewing attribute properties](#)
- [System information](#)

You can also view inventory data in reports that you generate. For more information, see [Reports overview](#).

## Viewing summary inventory from the local console

Summary inventory is found on the **Summary** page in the local console and provides a quick look at the device's basic OS configuration and system information.

---

**Note:** If you added a device to the core database using the discovery tool, its inventory data isn't yet scanned into the core database. You must run an inventory scan on the server for the summary inventory feature to complete successfully.

---

### To view summary inventory

1. In the console's **All devices** view, double-click a device. Or single-click a device to select it and click **Launch local console** from the **Properties** tab.
2. In the left navigation pane, click **Summary**.

### Windows 2000/2003 server summary data

This information appears when you view summary inventory for a Windows 2000/2003 server.

- **Health:** The current health state of the server.
- **Type:** The type of server, such as application, file, e-mail, and so forth.
- **Manufacturer:** The manufacturer of the server.
- **Model:** The server's model type.
- **BIOS version:** The version of the ROM BIOS.
- **Operating system:** Windows or Linux OS running on the server: 2000, 2003, or Red Hat.
- **OS Version:** Version number of the Windows 2000/2003 or Linux OS running on the server.
- **CPU:** Type of processor or processors running on the server.
- **Vulnerability scanner:** The version of the agent installed.
- **Remote control:** The version of the agent installed.
- **Software distribution:** The version of the agent installed.
- **Inventory scanner:** The version of the agent installed.
- **Last reboot:** The last time the server was rebooted.
- **CPU usage:** The percentage of the processor currently in use.
- **Physical memory used:** Amount of RAM available on the server.
- **Virtual memory used:** Amount of memory available to the server, including RAM and swap file memory.
- **Drive space used:** The percentage of drive space currently used. If you have more than one hard drive, each drive will be listed.

Servers that are IPMI-enabled display additional IPMI-specific data. Linux servers also display similar information in the **Summary** view.

## Viewing a full inventory

A full inventory provides a complete listing of a device's detailed hardware and software components. The listing contains objects and object attributes.

### To view a full inventory

1. In the console's **All devices** view, click a device.
2. In the **Properties** tab, click **View inventory**.

## Viewing attribute properties

You can view attribute properties for a device's inventory objects from the inventory listing. Attribute properties tell you the characteristics and values for an inventory object. You can also create new custom attributes and edit user-defined attributes.

To view an attribute's properties, click the attribute in the left pane.

To print this information in Internet Explorer, right-click in the frame and click **Print**. To print in Mozilla, right-click in the frame, click **This Frame | Save Frame As**, click **Save**, then open the file in an application and click **Print**.

## System information

From the local console, you can view and modify the device's system information. Information in the **Hardware**, **Software**, **OS event logs** and **Other** categories is either stored data or real-time data. When you click an information link you can view detailed information about the selected component and, in appropriate cases, set thresholds and enter information.

1. In the **All devices** list, double-click **My devices**.
2. In the console's **All devices** view, double-click a device. Or single-click a device to select it and click **Launch local console** from the **Properties** tab.
3. In the left navigation pane, click **System information**.
4. Click the information link you want to view.

## Customizing inventory options

The console includes a utility, SVCCFG.EXE, that you can use to customize inventory options. The defaults for most options should be fine, but if you need to change them, you can run SVCCFG.EXE from the core server's LANDesk\Server Manager\Program Files\LANDesk\ManagementSuite folder. You must run SVCCFG.EXE at the core server.

Use SVCCFG.EXE to configure:

- The database name, username, and password
- Device software scan interval, maintenance, days to keep inventory scans, and client login history length
- Duplicate device ID handling
- Scheduler configuration, including scheduled job and query evaluation intervals

- Custom job configuration, including remote execute timeout

Click **Help** on each SVCCFG.EXE tab for more information.

## Editing the LDAPPL3.TEMPLATE file

Information relating specifically to the scanner's inventory parameters is contained in the LDAPPL3.TEMPLATE file. This template file works with the LDAPPL3.INI file to identify a device's software inventory. This file is placed on managed devices as part of agent configuration. Its parameters are set in the Inventory tab of [Agent configuration](#).

You can edit the template file's [LANDesk Inventory] section to configure the parameters that determine how the scanner identifies software inventory. By default, LDAPPL3.TEMPLATE is located in the core server's LDLogon share.

Use this table as a guide to help you edit the [LANDesk Inventory] section in a text editor.

Option	Description
Mode	<p>Determines how the scanner scans for software on devices. The default is Listed. Here are the settings:</p> <ul style="list-style-type: none"> <li>• <b>Listed:</b> Records the files listed in LDAPPL3.</li> <li>• <b>Unlisted:</b> Records the names and dates of all files that have the extensions listed on the ScanExtensions line but that are not defined in the LDAPPL3. This mode helps discover unauthorized software on the network.</li> <li>• <b>All:</b> Discovers listed and unlisted files.</li> </ul>
Duplicate	Records multiple instances of files. Set the value to OFF to record only the first instance, or ON to record all detected instances. The default is ON.
ScanExtensions	Sets the file extensions (.EXE, .COM, .CFG, etc.) that will be scanned. Use a space to separate the file extensions. By default, only .EXEs are scanned.
Version	The version number of the LDAPPL3 file.
Revision	The revision number of the LDAPPL3 file; helps ensure future compatibility.
CfgFiles 1-4	<p>Records the date, time, file size, and contents of the specified files. You can leave out the drive letter (for example, c:) if you want to search all local drives. You can specify more than one file on each of the four lines, but the line length is limited to 80 characters.</p> <p>Separate path names on the same line by a space.</p> <p>The scanner compares the date and size of the current file with that of the previous scan. If the date and size don't match, the scan records the contents of the file as a new revision.</p>
ExcludeDir 1-3	Excludes specific directories from a scan. You can leave out the

- drive letter (for example, c:) if you want to exclude all local drives. Enumeration must start at 1 and be continuous. You must end each line with "\".
- MifPath** Specifies where MIF files are stored on a client's local drive. The default location is c:\DMI\DOS\MIFS.
- UseDefaultVersion** If set to TRUE, the scanner reports a match when a file matches an exact filename and file size entry in LDAPPL3 on filename only (the version will be reported as EXISTS). This can cause some false positives for applications that share a common filename with an unknown application. In the as-delivered LDAPPL3.TEMPLATE file, this parameter is set FALSE; that is, only add an entry if the match is exact. If the parameter is missing, it defaults to TRUE.
- SendExtraFileData** If set to TRUE, sends extra file data to the core server. The default is FALSE. This means that by default, only path, name, and version are entered into the core database.

#### To edit the LDAPPL3.TEMPLATE file

1. From your core server, go to the LDLogon directory and open LDAPPL3.TEMPLATE in Notepad or another text editor.
2. Scroll down to the parameter you're interested in updating and make your changes.
3. Save the file.

## Updating the application list

The data from the applications list, DEFAULTS.XML, is stored on the core database. Because the names and version numbers of commonly-used software applications change fairly often, LANDesk publishes a new DEFAULTS.XML several times a year (in versions of LANDesk software before 8.6, this file was LDAPPL.INI).

#### To update the application list

1. Download a new DEFAULTS.XML or LDAPPL3.TEMPLATE file from <http://www.LANDesk.com/support/downloads>. Select a product and click **Software update** to download the file.
2. Save the file to the LDLOGON directory.
3. Publish a new LDAPPL3.INI by following the steps in [Publishing the application list](#).

## Publishing the application list

Publishing the Application list involves importing the most current application list in DEFAULTS.XML into the database, and then combining the application list with the contents of LDAPPL3.TEMPLATE to generate an updated LDAPPL3.INI file. There is a standalone utility COREDBUTIL.EXE in the Management Suite directory which is used to automatically perform both of these steps.

**To publish the application list**

1. Start CoreDBUtil.exe
2. Click the **Publish App List** button.

You should publish the application list after modifying or downloading an updated version of LDAPPL3.TEMPLATE or DEFAULTS.XML.





# Software licenses

---

## Monitoring software license compliance

IT administrators often find it challenging to track product licenses installed on numerous devices across a network. They run the risk not only of over-deploying product licenses, but also of purchasing too many licenses for products that turn out to be unnecessary. You can avoid these problems by using software license monitoring to monitor product licenses and usage across your organization.

The power of compliance monitoring rests in its data-gathering capabilities. Use the data to track overall license compliance and to monitor product usage and denial trends. The software monitoring agent passively monitors product usage on devices, using minimal network bandwidth. The agent continues to monitor usage for mobile devices that are disconnected from the network.

Monitoring features include:

- Ability to scan for both known and unknown applications.
- Application launch denial to keep unauthorized software from running even on devices disconnected from the network.
- Full integration with the Web console for current, complete information about installed applications.
- Extensive application usage and license compliance reporting.
- Extensive license monitoring and reporting features, including number of times each licensed application was launched, last date used, and total duration of application usage.
- Easy configuration of license parameters, including number purchased, license type, quantity and serial number.
- License purchase information, including price, date purchased, P.O. number, and reseller information.
- Installation tracking and reconciliation, including the license holder and physical location of the device the license is installed on, as well as additional notes.
- Aliases to track software when vendor information or filenames change.

## How software license monitoring works

The software license monitoring agent, when installed, records the total minutes of usage, the number of launches and the last launch date of all installed applications on a device and stores this data in the device's registry at:

HKEY\_LOCAL\_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\Software Monitoring\MonitorLog

The device inventory scanner updates the core server with software license monitoring data when it does a software scan (by default, once a day). The inventory scanner uses a text file called LDAPPL3.INI to define which applications it should scan for. When the inventory scanner runs, it checks with the core server to see if the LDAPPL3.INI has been updated. If it has, the scanner gets the new version. The scanner uses file deltas and compression to minimize the amount of network traffic used. You shouldn't edit the LDAPPL3.INI file directly. For more information, see [Publishing the application list](#).

Application usage data that you don't monitor is eventually overwritten with newer data in the device's registry.

### About mobile devices

For mobile devices disconnected from the network, the Software Monitoring agent continues to record data and caches it in the device's registry. After the device reconnects to the network, the next scan detects which of the cached data is being monitored and sends that data to the core server.

## Software license compliance tree

The software license monitoring tabs are designed to let you monitor and manage the software that's installed on your devices. Navigate to these tabs by clicking **Software licenses** in the left navigation pane.

Use the **Compliance** tree to monitor usage and license compliance for products across your organization, set up product license downgrading, deny usage of applications on devices, and view license compliance, usage, and denied application trends.

Use the **All products** tree to see all predefined products and products you created.

## Creating product and vendor aliases

Use the **Aliases** tab to create product or vendor aliases. An alias ensures that you can correctly account for all installed products by:

- **Normalizing executable file data:** An alias lets you make consistent the information the core database needs to correctly identify an installed product. For example, the file information provided by a vendor isn't always consistent. Files scanned into the core database for various Microsoft products may show the vendor name as being Microsoft Corp, Microsoft (R), or just Microsoft. If you were to run a query on "Microsoft (R)" products, you would get only a partial list back of Microsoft products installed across your network. By creating a vendor alias of "Microsoft Corp" for all of your Microsoft products, you ensure that those products all have exactly the same vendor name.
- **Updating executable file data:** An alias lets you update file information if the product name or vendor changes after installation. For example, sometimes vendor or product names change because a company has been newly acquired or divested, or a company has renamed its product after several versions. If this occurs with your device applications, use aliasing to associate new vendor or product names with the originals, ensuring that the core database can continue to identify your executables accurately. This feature is especially useful if you're monitoring products in the Compliance tree and need to maintain accurate information about your licenses.

### About the Aliases tab

The Aliases tab shows the original vendor and name for a product, as well as any new vendor and/or product names that you may have added. A software scan must occur before a new alias will appear in the compliance tree.

You can create two types of aliases:

- **Vendor:** An alias for all installed products of a certain vendor (enter the original vendor name and a new vendor name).
- **Product:** An alias for a specific product (enter original vendor and product names, as well as new ones). A product alias that includes a new vendor will always take precedence over an alias created for all products of a certain vendor.

#### To create an alias

1. From the left navigation pane, click **Software licenses**.
2. On the **Aliases** tab, click **New**.
3. Enter the original vendor and original product name, as well as the new vendor and/or new product name for the application. You must enter information for all alias fields, even if the original and new values are the same.
4. Click **OK**.

To edit an existing alias, click the alias and click **Edit**. To delete an alias, click the alias and click **Delete**. After you delete an alias, the database reverts to using the original vendor and product name after the next software scan.

## Monitoring products for compliance

### Setting up a product

The **Compliance** tree view contains a hierarchical tree of product groups and individual products. You can group products any way you want, for example:

- By company, such as Adobe\* or Microsoft\*
- By specific categories, such as Unauthorized Files or Accounting Department
- By product suite, such as Microsoft Office

Within these groups, add the products that you want to monitor for usage or denial trends. For example, under an Adobe group, you might add products such as Photoshop\* and Illustrator\*.

The **All products** tree view shows all predefined products and products you created. Drag products from this view into the compliance view so you can configure them for monitoring.

#### To set up a product

1. In the left navigation pane, click **Software licenses**.
2. If don't want to use an existing product group in the compliance tree, create one as described in [Managing product groups](#). You can only add products to a group.
3. Click the group you want to create the product in. Click the **New** toolbar button.
4. Enter the product information, as described in [Managing products](#).
5. Continue configuring the product by following the steps in [Selecting product files to monitor](#).

6. Add license information by following the steps in [Adding product license information](#).
7. Export the LDAPPL3.INI by following the steps in [Customizing and exporting LDAPPL3.INI](#)

## Managing product groups

The **Compliance** tree view contains a hierarchical tree of product groups and individual products. You can group products any way you want, for example:

- By company, such as Adobe\* or Microsoft\*
- By specific categories, such as Unauthorized Files or Accounting Department
- By product suite, such as Microsoft Office

Within these groups, add the products that you want to monitor for usage or denial trends. For example, under an Adobe group, you might add products such as Photoshop\* and Illustrator\*. You can only add products to a group, and groups can't be nested.

### To add product groups

From the left navigation pane, click **Monitor software**. In the **Compliance** tree view, do one of the following:

- To add a product group: Click the **Compliance** tree item, then click **New**. Enter the new group name and click **OK**.
- To edit a product group name: Click the **Compliance** tree item, and in the right pane click the group you want to edit. Click **Edit**. Enter the new group name and click **OK**.
- To delete or rename a product group or product: Click the **Compliance** tree item, and in the right pane click **Delete**. In the confirmation dialog, click **OK** to delete the group.

## Managing products

You can add software license monitoring products under a product group. Create a new group or select an existing group for the product you want to add, as described in [Managing product groups](#). Once you've clicked on a group and entered the product view, you can do the following:

- **Add a product:** Under the **Compliance** tree item, click the group you want to add the product to. Click the **New** button and select an existing product from the **Product list**, or enter a **Product name**.
- **Edit a product:** Under the **Compliance** tree item, click the group you want to edit a product in. In the right pane, click the product and click the **Edit** button. You can change the product name and check or clear the **Match all files** option.
- **Delete a product:** Under the **Compliance** tree item, click the group you want to delete a product in. In the right pane, click the product and click the **Delete product** button. When you delete a product it deletes the product from the tree view. Deleting a product doesn't remove files you specified as being part of the product from the main software file list.

The product dialog also allows you to choose the **Match all files** option. By default, the presence of any file in the **Product files** list will be considered a product match.

The **Match all files** option requires all files be present on the client. For more information, see [Tracking licenses using the match all files option](#).

## Managing denied products

The denied products tree item doesn't allow groups. Instead, add, edit, and delete products at the root level. You can do this by clicking **Denied products** and then clicking the button that matches what you want to do. For more information on denied products, see Denying product execution.

## Selecting product files

Use the a product's **Files** pane to specify which files should be monitored to determine when a product is running.

If you selected the **Match all files** option in the product properties dialog, all files you select must be on the device for software license monitoring to register a match. If you don't select the **Match all files** option, the presence of any file in the list on a device is considered a product match.

For denied products, the Match all files option is ignored. All files in a denied product will be blocked. For more information, see Denying product execution.

If you're tracking different products that use the same file, you need to treat the products sharing the file differently. For example, if you're tracking license usage for MSDE and SQL 2000, and they both use SQLSERVER.EXE of the same size, you should also track a .DLL or other application file that's unique to each product. The Web console won't monitor these other files for compliance (only executables are monitored for compliance), but the unique file will help the scanner distinguish the MSDE license from the SQL 2000 license.


---

If you add files to a product other than .EXEs, you must first edit the LDAPPL3.TEMPLATE file to include those files in a software scan. Information relating specifically to the scanner's inventory parameters is contained in the LDAPPL3.TEMPLATE file. This template file works with the LDAPPL3.INI file to identify a device's software inventory. By default, LDAPPL3.INI only scans for executables. For more information, see [Editing the LDAPPL3.TEMPLATE file](#).

---

### To select files to monitor

1. In the left navigation pane, click **Software licenses**.
2. In the tree, click **Compliance | product group | product name / Files**. If you're working with a denied product file list, instead click **Denied products**.
3. Click the **Add** toolbar button.
4. In the **File** dialog, enter a filter string. You don't have to enter the full file name, and you can use an asterisk as a wildcard character.
5. Select the inventory column you want to search in, either Any, Vendor, Product name, File name, Version, or Size.
6. Select the file list you want to search in, either All, Discovered, or Not in product.
  - **All:** All predefined files in the LDAPPL3.INI (even if they haven't been discovered on devices), and all files that have been discovered on devices.

- **Discovered:** Only files that have been discovered on devices, even if they're for products that aren't defined in the LDAPPL3.
  - **Not in product:** All files that aren't currently being monitored in the Compliance tree. Use this list to search for files that you may want to begin monitoring for license compliance and usage/denial trends. This view doesn't include files on the denied list.
7. Click the search button  beside the **In column** list to begin your search. Depending on the number of matches, it might take a while for the results to appear.
  8. Click the files that indicate this product's presence on devices.

---

If the list of files spans multiple pages, use the arrows at the top of the page to navigate between pages. Enter the number of items to display per page and click **Set**.

---

## Tracking licenses using the match all files option

Normally, software license monitoring considers the presence on a device of any file in the product's **Files** list of files a product match. You may encounter a situation where you need to track licenses for two or more products that contain an executable of the same name and size. In such a case, you also need to monitor a file unique to each product. By checking **Match all files** in the **Product dialog** and using both the executable and a unique file to identify license usage, you specify that all files associated with a product (as found in the **Product files** pane) need to be installed on a device before a product license is considered used. This ensures that the scanner can correctly track the products licenses.

The following two examples help explain when you would check **Match all files**:

- If you're tracking license usage for MSDE and SQL 2000, and they both use SQLSERVER.EXE of the same size, you should also track a .DLL or other application file that's unique to each product. The Web console won't monitor these other files for compliance (only executables are monitored for compliance), but the unique file will help the scanner distinguish the MSDE license from the SQL 2000 license.

---

If you add files to a product other than .EXEs (in order to use the Match All Files option), you must first edit the LDAPPL3.TEMPLATE file to include those files in a software scan. By default, LDAPPL3 only scans for executables. For more information, see [Editing the LDAPPL3.TEMPLATE file](#).

---

- If you're monitoring 10 licenses for Office XP Standard (that includes Word, Excel, Outlook, and PowerPoint), as well as 10 licenses for Office XP Pro (that includes the same applications, in addition to Access), you face the problem of wanting to monitor two distinct product licenses that contain executables of the same name and size. The scanner can't distinguish between license types by tracking individual files, nor by using just the **Match all files** option for both products.

In this case, you must go one step further by adding an Office XP Pro executable to the **Product files** pane of XP Standard (for example, Access) and marking that executable as **Exclude from product**. This ensures that the software monitoring agent won't record an Office XP Pro license as an XP

Standard license, which would occur if only **Match all files** was checked. For more information on marking a file as excluded, see [Selecting product files to monitor](#).

## Adding product license information

You must add license information to monitor a product for license compliance. If you only want to track product usage, you can skip this procedure.

After you set up license information for a product, if you ever see a red icon with an exclamation point appearing next to the product group, this means that one of the products in the group isn't license-compliant. Expand the product group to find the non-compliant product, then view its associated information in the right pane.

### To add product license information

1. Click **Software licenses**.
2. In the **Compliance** tree, click *product group | product name / Licenses*.
3. Click the **New** toolbar button.
4. In the **License** dialog, enter the license, purchase, and tracking information that's relevant to your organization.
5. When finished, click **OK**.

---

To ensure that all executables associated with a product are installed on a device before that product's license is monitored for compliance, right-click the product name in the right pane and click **Edit product**. In the **Product** dialog, make sure **Match all files** is checked. For more information, see [Tracking licenses using the match all files option](#).

---

## About the License Properties dialog

The License Properties dialog has three tabs:

- License
- Purchase Info
- Tracking

Use the License tab to configure license properties for your product.

- **License number:** Enter a number that constitutes your product license.
- **License type:** Enter a type of license you have for the product, such as: competitive upgrade, freeware, new purchase, OEM, product upgrade, public domain, shareware, unknown.
- **Quantity:** Enter the number of product licenses purchased.
- **Serial number:** Enter an additional number that may constitute your product license.

Use the Purchase Info tab to configure purchase properties for your product license.

- **Purchase date:** Enter a date the product was purchased by your company.
- **Unit price:** Enter a price of each purchased license for the product.
- **Order number:** Enter an order number used to make the purchase.



- **Reseller:** Enter the name of purchase place.

Use the Tracking tab to configure tracking properties for your product license.

- **Owner:** Enter a person or department in your company responsible for storing the boxed product.
- **Location:** Enter a physical location where the boxed product is stored.
- **Notes:** Enter any additional information associated with the product license, such as downgrade rights.

## Denying product execution

You can prevent devices from executing files you specify. When devices try to run a denied product, the product won't launch on their system and they'll see a message box telling them their system administrator has prevented access to that program.

You can restore normal access to a product by deleting the product in the **Denied products** group. Deleting a product here doesn't actually delete the product. It only removes the product from the group.

All files in **Product files** list for a denied product will be denied on devices. The **Match all files** product option state doesn't affect denied products.

You must publish the LDAPPL3.INI and devices must receive the updated version before changes take effect. For more information, see [Publishing the application list](#).

## Resetting usage data

If you ever want to clear the data for your monitored products' usage or denial reports, you can. Clearing the data lets you reset the counter so you can begin tracking applications from a certain point on. The reset affects all devices, and it clears the device registries and the core database of all past usage and denial report data. For this reason, it's important to print or save any usage or denial reports you may want to keep before resetting. When you reset the usage and denial report data, you do so for all monitored products in the Compliance tree.

### To reset usage and denial report data

1. From the left navigation pane, click **Software licenses**.
2. In the lower pane, click the **Reset usage** tab.
3. Click **Next** to complete the reset.

After you reset, you'll need to force a scan to clear the report data from your device registries, then you'll have to force a second scan before the new data is actually recorded in the Software License Monitoring window.

On large databases, the reset can take a long time. If the reset times out, your DBA can reset the usage manually by entering these SQL commands:

```
UPDATE FileInfoInstance
SET SCM_TotalSessionTime = NULL,
SCM_SessionCount = NULL,
SCM_SessionsDenied = NULL,
SCM_LastUser = NULL,
```

```
SCM_LastSessionTime = NULL
```

## Publishing the application list

The device inventory scanner uses an application list called LDAPPL3.INI that contains software inventory information. The LDAPPL3.INI is populated initially with most popular application executable filenames and file information. When the scanner runs on devices, it uses a local LDAPPL3.INI copy to match device executable filenames with the software inventory information.

The master LDAPPL3.INI resides in the core server's LDLogon share. Whenever you make a change to the application list, you must export a new LDAPPL3.INI file. When you export a new LDAPPL3.INI, the core server uses the LDLogon share's LDAPPL3.TEMPLATE text file to create the framework for the exported LDAPPL3.INI. The core server then populates this framework with file information from the core database. Finally, the core server writes the exported LDAPPL3.INI file to the LDLogon share, replacing any existing version. The next time servers do a software scan, they automatically receive the updated LDAPPL3.INI.

By default, LDAPPL3.INI contains descriptions of executables only. If you want the scanner to also identify other types of application files (.DLLs, .COMs, .SYSes, and so on), you can edit the LDAPPL3.TEMPLATE file to include all files of that type in a scan. For more information, see [Editing the LDAPPL3.TEMPLATE file](#).

You shouldn't edit the LDAPPL3.INI directly in a text editor, because the data is stored in the core server's core database. The next time the server writes a new version of this file, changes made directly with an editor will be lost. All changes to the LDAPPL3.INI should be made in the LDAPPL3.TEMPLATE file.

### To publish a new application list

After changing the application list by [editing the LDAPPL3.TEMPLATE file](#), publish a new LDAPPL3.INI by following the steps below.

1. From the left navigation pane, click **Software licenses**.
2. In the lower pane, click the **Publish list** tab.
3. Click **Next**.

Changes you make won't take effect on devices until they receive the updated LDAPPL3.INI.

### Making the LDAPPL3.INI file available to devices

Each device that runs the inventory scanner has a local copy of LDAPPL3.INI. The devices' LDAPPL3.INI is initially installed as part of the default device configuration setup. Both the device and core version of this file must be synchronized for the scanner to know which files to scan or deny on devices. The core server and device LDAPPL3.INI synchronization uses delta matching so only the changes are transmitted. File compression further reduces the core's LDAPPL3.INI by 70 percent, which enables the scanner to update the devices' corresponding LDAPPL3.INI without using significant bandwidth.

If you don't want to wait for the next inventory scan to update your device LDAPPL3.INI files, you can make the edits available to devices by scheduling a job to push LDAPPL3.INI down to devices.

# Core database installation and maintenance

---

## Installing an SQL or Oracle database

The default installation uses a Microsoft MSDE database on your core server. If you aren't planning to use a default MSDE database on your core server, you need to set up a database before running Setup. During Setup, you'll point to the database that will hold your data.

The database schema supports these databases:

- Microsoft SQL Server 2000 with SP 4
- Oracle8i (8.1.7). Requires Oracle's OLE DB version 8.1.7.3 update.
- Oracle9i

All database servers need to have MDAC 2.8 on them.

---

### If you have a preexisting Windows 2000/2003 master domain

Don't install the database to the primary domain controller (PDC). The database should be installed only on a standalone server. You can install the database on the backup domain controller (BDC) in a small Windows 2000/2003 domain, but Server Manager doesn't recommend it.

---

## Microsoft SQL Server 2000 configuration

The console core server needs the following parameters. These parameters will be set by default if you use a typical install for SQL 2000.

### SQL server configuration parameters

- Microsoft SQL 2000 performs self-tuning. You shouldn't need to tune any parameters manually.

### Database parameters

- Use the defaults.

### Other settings

- Use sa or another user aliased into the database as DBO when creating the database.
- Set up database maintenance.
- Make sure that Microsoft Internet Explorer 6 SP1 or newer is installed.

### To install the console so that it uses your SQL 2000 database

1. Install to the point where you need to choose a database. Click **User-supplied database**, then click **Next**.

2. In the Server field, enter the database server name for the SQL database. In the Database field, enter the database name. In the User field, enter the database user name. In the Password field, enter the database password. Click **Next**.
3. If the database you entered is currently populated, you will be prompted to reset the database. Click **Yes** to reset the database or click **No** to keep the existing database information.
4. Finish the console install.

## SQL maintenance

You must regularly perform maintenance on a Microsoft SQL Server database. Over time, the indexes become very inefficient. If your database includes a large number of managed servers and queries seem to be running more slowly than normal, updating statistics on all tables within the database can substantially improve query performance. On very large databases, you might want to update statistics daily.

Microsoft SQL maintenance requires the SQLServerAgent service to be running on the SQL server. You may need to set the service to Automatic in the Control Panel Services applet. SQL maintenance won't run unless the SQLServerAgent service is started.

### To set up a maintenance task

1. Click **Start | Programs | Microsoft SQL Server | Enterprise Manager**.
2. Click the + next to these folders: **Microsoft SQL Servers**, **SQL Server Group**, **the name of your server**, and **Management**.
3. Right-click **Database Maintenance** and click **New Maintenance Plan**.
4. In the **Database Maintenance Plan** dialog, click **Next**.
5. In the **Select Databases** dialog, select **These databases** and select the checkbox for your database. Click **Next**.
6. In the **Update Data Optimization Information** dialog, click **Reorganize data and index pages**.
7. Set the **Change free space per page percentage** to option to **10**.
8. Click the **Change** button next to the **Schedule** window.
9. In the **Edit Recurring Job Schedule** dialog, select the schedule you want for maintenance. We suggest you perform the maintenance at least weekly at a time when there will be minimal database activity.
10. Click **OK**.
11. In the **Database Integrity Check** dialog, select these options: **Check database integrity** and **Include indexes**, and click **Next**.
12. In the **Specify the Database Backup Plan** dialog, specify your own backup schedule and click **Next**.
13. In the **Specify the Transaction Log Backup Plan** dialog, specify your own backup schedule and click **Next**.
14. In the **Reports to Generate** dialog, select the **Write report to a text file in directory** option and click **Next**.
15. In the **Maintenance Plan History** dialog, select the **Write history to the msdb.dbo.sysdbmaintplan\_history table on this server** option.
16. Set the **Limit rows in the table** to option to **1000**.
17. Click **Next**.

18. In the **Completing the Database Maintenance Plan** dialog, enter a **Plan name** and click **Finish**.

## Oracle database configuration

The default Oracle client installation installs Apache, disables IIS, and makes Apache the default Web server. The Web console server requires IIS. If you're doing a full Oracle client installation on the core server or the Web console server, make sure you disable the Apache feature in the client installer.

In Oracle, this product uses public synonyms. After installing an Oracle database, do the following:

1. Create a tablespace for Setup to use.
2. Create a user with the following system rights for Setup to use:
  - Create Procedure
  - Create Sequence
  - Create Session
  - Create Table
  - Create Trigger
  - Create Type
  - Create View
  - Force Transaction
  - Unlimited Tablespace
3. Set the user's default tablespace to the tablespace created for Setup's use.
4. On the core server, create a TNS entry for the Oracle instance.

## Oracle performance tuning suggestions and scripts

Like any DBMS, Oracle should be tuned to help increase performance. The first step in increasing performance is to make sure sufficient hardware is allocated for the Oracle instance.

If your database includes a large number of servers and queries seem to be running more slowly than normal, updating statistics on the all tables and indexes in the database can substantially improve query performance. On very large databases, you might want to update statistics daily.

## Miscellaneous Oracle issues

The following sections contain specific issues that you should review to get optimal performance when using an Oracle database.

You must install Oracle Windows Interfaces on the core machine with the Oracle ODBC driver and the Oracle provider for OLE database.

### TNS Names

Use Oracle's SQL Net Easy Configuration tool to create a TNS entry on the core server that points to the physical location of the Oracle database. The configuration tool adds an entry into the \$ORACLE\_HOME/Network/ADMIN/TNSNames.ora file. Because each console relies on the core server to provide a database connection string, and because Oracle uses TNS names, each console must have the Oracle client installed with an identically named TNS name that exists on the core server. You must run the SQL Net Easy Configuration tool on each console to set up a TNS name.

### You must create an Oracle TNS name entry on the core

If you don't create an Oracle TNS name entry on the core computer, the core won't be able to communicate with the database.

### If services fail to start using Oracle

If the LANDesk services are failing to start and checking the event log shows errors about "Adapter initialization failures" or "Adapter Authentication failures," change the following file:

\$ORACLE\_HOME/network/admin/sqlnet.ora

Change:

SQLNET.AUTHENTICATION\_SERVICES = (NTS)

To:

SQLNET.AUTHENTICATION\_SERVICES = (NONE)

### Using Oracle 9.2.0.1 with the console

If you use an Oracle 9.2.0.1, there is an Oracle install bug that doesn't set the proper permissions for authenticated users (which IIS uses). If you see a Web console error about not being able to authenticate to the database, follow these steps to fix it.

1. Log in to Windows as a user with administrator privileges.
2. Launch Windows Explorer from the Start menu and navigate to the ORACLE\_HOME folder. This is typically the "Ora92" folder under the "Oracle" folder (i.e. D:\Oracle\Ora92).
3. From the ORACLE\_HOME folder's shortcut menu, click **Properties**.
4. Click the **Security** tab.
5. In the **Name** list, click **Authenticated Users**.
6. In the **Permissions** list under the **Allow** column, clear the **Read and Execute** option.
7. Re-check the **Read and Execute** option under the **Allow** column (this is the box you just cleared).

8. Click **Advanced** and, in the **Permission Entries** list, make sure you see the **Authenticated Users** listed there with Permission = Read & Execute and Apply To = This folder, subfolders and files. If this isn't the case, edit that line and make sure the **Apply onto** box is set to **This folder, subfolders and files**. This should already be set properly, but it's important that you verify this.
9. Click the **OK** until you close out all of the security properties windows.
10. Reboot your server to make sure that these changes have taken effect.

## Using rollup databases

The database Rollup Utility (DBROLLUP.EXE) enables you to take multiple source core databases and combine them into a single destination core rollup database, allowing you to create reports or query the managed devices across your organization. . A core server database can support several thousand devices, and the rollup core device limit depends on your hardware and acceptable performance levels. The source database can be either a core server or a rollup core server.

The system requirements for a destination database may be substantially greater than the system requirements for a standard database. These requirements can vary considerably depending on your network environment. If you need more information about hardware and software requirements for your destination database, contact your LANDesk Software support representative.

Setup installs the database Rollup Utility automatically with the rollup core. The Rollup Utility uses a pull mechanism to access data from cores you select. For database rollups to work, you must already have a drive mapped to each core you want the Rollup Utility to get data from. The account you connect with must have rights to read the core server's registry.

The Rollup Utility checks with a registry key on the core server for database and connection information (HKLM\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\local) and uses that key's information to access the database associated with each core you add to the Rollup Utility. For Oracle databases, the TNS definition on the server you're running the Rollup Utility from must match the TNS definition on the core server the utility is accessing.

You can use the rollup utility to select the attributes you want rolled up from the cores. The attribute selections you make apply to all cores. Limiting the number of attributes shortens the rollup time and reduces the amount of data transferred during rollups. If you know you won't be querying on certain attributes, you can remove them.

The Rollup Utility always rolls up the selected attribute data and Software License Monitoring data. You can't customize the Software License Monitoring rollup. Rollup also doesn't include any queries or scopes you've defined. Any console users with rights to the rollup database have access to all data within that database.

Once you've added the core servers you want to roll up and the attribute list for those servers, you can click Schedule to create a scheduled rollup script for each core server. From the rollup core's Web console, you can then schedule these rollup scripts to run at the time and interval you want. Rollup scripts on the rollup core.



**To launch the Rollup Utility**

1. On a rollup core, run the Rollup Utility (\Program Files\LANDesk\ManagementSuite\dbrollup.exe).
2. Select an existing rollup core server to manage from the list, or click **New** to enter the name of a new rollup core server. Note that you must enter the core server name, and not the database name.
3. Once you select a rollup core, the Source cores list shows cores you've configured to roll up to the selected rollup core.

**To configure the attributes that you want to roll up**

1. From the Rollup Utility, select the rollup core you want to configure.
2. Click **Attributes**.
3. By default, most database attributes are rolled up. Move attributes that you don't want to roll up from the **Selected Attributes** column back to the **Available Attributes** column.
4. Click **OK** when you're done. Moving attributes to the **Available Attributes** column deletes associated data from the rollup database.

**To configure the source core servers for a rollup core**

1. From the Rollup Utility, select the rollup core you want to configure.
2. Once you select a rollup core, the Source cores list shows cores you've configured to roll up to the selected rollup core. Click **Add** to add more cores or select a core and click **Delete** to remove one.

**WARNING:** Clicking delete immediately removes the selected core and all of that core's data from the rollup core database. Also, if you supply an invalid link name when adding a core server to the rollup database, you will have to remove the core from the rollup and re-add it in order to modify the link name.

**To schedule database rollup jobs from the Web console**

1. From the Rollup Utility, select the **Rollup core** you want to configure.
2. In the **Source cores** list, select the cores you want to schedule for rollup and click **Schedule**. If you don't select any cores, by default all cores in the list will be scheduled when you click **Schedule**. Clicking **Schedule** adds a rollup script for the selected core to the selected rollup core. If you select multiple cores, they will be scheduled as one job and will be processed one at a time.
3. You won't be able to log into a rollup core server from the Web console until at least one core has been rolled up to it. Make sure you use the Rollup Utility's **Rollup** button to manually roll up at least one core.
4. From a Web console, connect to the rollup core server (<core name>/ldsm/).
5. In the left navigation pane, click **Scheduled tasks**.
6. Click the rollup script you want to schedule. The script names begin with the source core name followed by the destination rollup core name in parentheses (such as *sample name*).
7. Click **Edit**.
8. Select when you want the roll up to happen and whether it should automatically reschedule or not. When scheduling recurring rollup tasks, make sure there isn't more than one core being rolled up at the same time.

9. Click **Save**.

You can view the rollup task status in the **Status** column. The column displays **All Completed** when the task is finished. )You can also view the status of the task in the Windows Event Viewer.)

Only one rollup can be processed at a time. A scheduled rollup will fail if another rollup is already in progress. When scheduling rollups, allow enough time between rollups that there won't be any overlap. If the rollup times are hard to predict, it's best to schedule all the rollups in a single task. Do this by targeting multiple cores before scheduling. This way, the rollups are handled one at a time automatically.

## Increasing the rollup database timeout

With large rollup databases, the Web console's query editor may time out when it tries to query and display a large list, such as the Software Package Name list. When this happens, the list you are trying to display won't show any data. If you experience timeouts you need to increase the database timeout value on the core running the IIS service or the Web console server. At the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core`

Add a new DWORD, Timeout, with a decimal value of 1800. This value is in seconds. You can adjust this value based on your query types and database performance. Stop and restart the IIS service for the change to take effect.

## About the Rollup Utility

Use the database Rollup Utility (run from the rollup core) to manage data rollups from core servers. A rollup core hosts the consolidated data from multiple LANDesk core databases.

- **Rollup core:** You can manage multiple rollup cores from the Rollup Utility. Select the core(s) you want to manage. You first must have a drive mapped to each rollup core.
- **New:** Click to add a new rollup core that you want to manage from the utility. You first must have a drive mapped to the rollup core you're adding. Enter the rollup core's computer name and click **OK**.
- **Attributes:** Click to select the attributes you want rolled up. The attributes list is global for all core servers the selected rollup core uses. Move individual attributes or attribute trees from the **Selected Attributes** column (these attributes will be rolled up) to the **Available Attributes** column (these attributes won't be rolled up).
- **Reset database:** Click to reset the selected rollup database. This deletes all data and rebuilds all tables.
- **Add:** Click to add a core that you want to include data from in the selected rollup core.
- **Delete:** Click to remove the selected core and its data from the selected rollup core's database. **WARNING:** This option deletes the selected core's data from the rollup core when you click **OK**. Data from other core servers remains in the rollup database.
- **Schedule:** Click to add a rollup script for the selected core. If you don't have a core selected in the Source Cores box, this option creates rollup scripts for all cores in the Source Cores box.
- **Rollup:** Click to do an immediate rollup from the selected core. You must have a core selected for this option to be available.
- **Close:** Click to close the Rollup Utility.

## Configuring rollup database links

This section describes how to configure database links in all four LANDesk software rollup scenarios. The four scenarios are:

- [Oracle rolling to Oracle](#)
- [SQL Server rolling to SQL Server](#)
- [SQL Server rolling to Oracle](#)
- [Oracle rolling to SQL Server](#)

The person doing this configuration must also have access to all DBMSs used by LANDesk, and they must have security permissions to create database links and perform configuration steps at a DBMS server level.

### Oracle rolling to Oracle

#### Configuring the Oracle database

The TNSNames.ora file on the database server in which your rollup database exists must contain an entry for your core server database.

1. For an Oracle 9i\* database, within the Enterprise Manager Console, log in to your database. Expand **Distributed**. For an Oracle 8i\* database, within the Enterprise Manager Console, log in to your database. Expand **Schema** and your rollup Schema.
2. From the **Database Links** item's shortcut menu, click **Create**.
3. In the **Name** field, enter a name for your database link. **Note:** In the name, LDMS\_LINK is the name of the link. If the AR database is using Oracle8i, the link name must match the TNS name of the remote server. If the AR database is using Oracle 9i, the link name can be any name that is not already in use or is reserved. The installation will prompt you for this information.
4. Choose **Fixed User** and enter the username and password for the core server's database.
5. In the **Service Name** field, enter the TNSNames.ora (i.e....Net Alias) entry that refers to your core server database.
6. Click **Create**.
7. Double-click your newly-created link and click the **Test** button. You should get a message that says your link is active. You can also test your link by logging into the rollup database and typing the following command:

```
Select count(*) from computer@linkname;
```

If it comes back with the correct number of computers scanned into your core server, your link is set up correctly.

## SQL Server rolling to SQL Server

### Configuring the SQL Server\* database

1. Open SQL Server Enterprise Manager.
2. Expand your server and click **Security**.
3. From the **Linked Servers** item's shortcut menu, click **New Linked Server**.
4. On the **General** tab, do steps 5-11:
5. **Linked Server**: enter a unique name for this database link (for example, LDMS core server1 Link).
6. Choose **Other** data source.
7. Select **Microsoft OLE DB Provider for Microsoft SQL Server**.
8. **Product name**: leave blank.
9. **Data source**: enter the name the database server containing the core database.
10. **Provider string**: enter your provider string. For instance:

```
SQL Server provider=SQLOLEDB.1;user id=<username for the core
server's database>
```

11. **Catalog**: enter the physical name of your core server's database (for example, lddb).
12. On the **Security** tab, do steps 13-14:
13. Select **Be made using this security context** and enter the username and password for the core server's database, then click **OK**.
14. Open SQL Query Analyzer and type the following command:

```
Select count(*) from [Link name].[database name].[table-owner
name].Computer
```

Using the values above, this query would appear as:

```
Select count(*) from [LDMS Core Server1
Link].[lddb].[dbo].Computer
```

If the correct count comes back, your link is set up correctly.

## SQL Server rolling to Oracle

### Configuring SQL Server to rollup to Oracle

In order to roll SQL Server to Oracle, you must capitalize all column names in the production SQL database. If you want a utility to do this for you, call LANDesk customer support.

### Install Heterogeneous Services for Oracle

1. Using the Oracle Universal Installer, Install the **Oracle Transparent Gateways** for SQL.
2. Edit <oracle home>\rdbms\admin\caths.sql on the Oracle DBMS server so that the two lines that call PRVTHS.PLB and DBMSHS.SQL point to the appropriate directory on Oracle DBMS server.

3. Execute CATHS.SQL using SQL Plus by logging in to SQL Plus and at the prompt typing:

```
@@$ORACLE_HOME/RDBMS/ADMIN/CATHS.SQL.
```

The following error may appear at the end script execution.

```
068: existing state of packages has been discarded
063: package body "LDPROD.DBMS_HS_UTL" has errors
508: PL/SQL: could not find program unit being called
512: at "LDPROD.DBMS_HS", line 629
403: no data found
512: at line 6
```

This error can be caused by an outdated version of JDBC drivers that exists on the Oracle DBMS server. Please call Oracle for troubleshooting and further investigation of your installation if you receive errors during the execution of CATHS.SQL or the scripts that it may call.

### Create a UDL file on the core server pointing to the SQL DBMS

1. Create a .UDL file on the core server by right-clicking on the desktop and clicking **New | Text Document**. Save it as <core server name>.udl. Double-click the .udl file and the **Data Link Properties** dialog displays.
2. On the **Data Link Properties** dialog's **Provider** tab, click **Microsoft OLE DB Provider for SQL Server**.
3. On the **Data Link Properties** dialog's **Connection** tab, fill in the database information for the core server's SQL Server database. Click **Allow Saving Password** to save the password information to the UDL file.
4. Click **OK** on the **Data Link Properties** dialog to save the connection information. When prompted whether or not to save the password, click **Yes**.

### Create a SID on the Oracle server pointing to SQL Server

1. Copy the ORACLE\_HOME/hs/admin/inithsoledb.ora and rename it to init<core server Name>.ora. Copy the UDL file created on the core to ORACLE\_HOME/hs/admin.
2. Edit the init<Core Server Name>.ora file. Change the HS\_FDS\_CONNECT\_INFO= line to reflect the path to your UDL file on the Oracle DBMS server. Leave the %\_TRACE\_LEVEL = 0 parameter equal to 0.
3. Save the init file and close it.
4. Create a listener pointing to the SQL Server by editing the Listener.ora and TNSNAMES.ORA files under ORACLE\_HOME/Network/Admin on the Oracle DBMS server.

Sample Entry for TNSNAMES.ORA:

```
<Core Server Name> =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = <Oracle DBMS server>
Name)(PORT = 1521))
  )
  (CONNECT_DATA =
```

```

        (SID = <Name of core server>)
    )
    (HS = OK)
)
Sample Entry for LISTENER.ORA
(SID_DESC =
    (GLOBAL_DBNAME = <Name of core server>)
    (PROGRAM = hsolesql)
    (SID_NAME = <Name of core server>)
    (Oracle_HOME = E:\oracle\ora92)
)

```

5. Restart the Listener Service on the Oracle DBMS server so that the Oracle server will now be able to connect to the SQL Server using OLEDB and Transparent Service.

### Create a Database Link using the core server-named SID.

Use the Core Server Name entry in TNSNames.ora file for the Heterogeneous Services link in order to create your link to your SQL Server production database.

1. For an Oracle 9i database, within the Enterprise Manager Console, log in to your database. Expand **Distributed**. For an Oracle 8i database, within the Enterprise Manager Console, log in to your database. Expand **Schema** and your rollup Schema.
2. From the **Database Links** item's shortcut menu, click **Create**.
3. In the **Name** field, enter a name for your database link.
4. Choose **Fixed User** and enter the username and password for the core server's database.
5. In the **Service Name** field, enter the TNSNames.ora (i.e....Net Alias) entry that refers to your core server database.
6. Click **Create**.
7. Double-click your newly-created link and click the **Test** button. You should get a message that says your link is active. You can also test your link by logging into the rollup database and issuing the following command:

```
Select count(*) from computer@linkname;
```

If it comes back with the correct number of computers scanned into your core server, your link is set up correctly.

8. You can also create your link by logging into SQL Plus for Oracle and typing the following SQL statement:

```
create database link "<core server Name(this will be the
linkname)>" connect to "<sql user name>" identified by
"<password>" using '<core server Name(this is the SID name)>';
```

## Oracle rolling to SQL Server

### Configuring Oracle to rollup to SQL Server

Because of a known issue in the Oracle 9i client, it is impossible to use DBROLLUP.EXE to roll an Oracle production database to an SQL Server rollup database using the Oracle 9i client.

It is possible to use the Oracle 10G client to roll an Oracle 9i database to SQL Server. Currently, the Oracle 10G client is not supported in conjunction with LANDesk Management Suite. It can be used though in conjunction with DBROLLUP.EXE in order to allow rollup of an Oracle database to SQL Server based upon the following limitations:

- The Oracle 10G client can't be installed on any server that houses a LANDesk core server, LANDesk additional console, or LANDesk web console server.
- The Oracle 10G client can only be used to point to an existing supported LANDesk production Oracle 9i database.

### Create a link to the Oracle database in SQL Server

1. Install the Oracle 10G on the rollup server.
2. Create an Oracle Net Alias to the production Oracle database. The Alias name must be the same as the Alias name used on the core server that uses that database.
3. Open SQL Server Enterprise Manager.
4. Expand your server and click **Security**.
5. From the **Linked Servers** item's shortcut menu, click **New Linked Server**.
6. On the **General** tab, do steps 7-12:
7. **Linked Server**: enter a unique name for this database link (for example, LDMS Core Server1 Link).
8. Choose **Other** data source.
9. Select **Oracle Provider for OLE DB**.
10. **Product name**: leave blank.
11. **Data source**: enter the name the database server containing the core database.
12. **Provider string**: enter your provider string. For instance:

```
provider=ORAOLEDB.ORACLE.1
```

13. On the **Security** tab, do steps 14-15:
14. Select **Be made using this security context** and enter the username and password for the core server's database, then click **OK**.
15. Open SQL Query Analyzer and issue the following command:

```
Select count(*) from [Link name]..[Oracle User Name].COMPUTER
```

Using the values above, this query would appear as:

```
Select count(*) from [LDMS Core Server1 Link]..[Oracle User Name].COMPUTER
```

If the correct count comes back, your link is set up correctly.

## Multi-core support

The following conditions must be met in order to use multiple cores:

- Both cores must be part of the same domain.
- The domain administrator account must be added the LANDeskManagementSuite local user group on both cores.
- The identity of the LANDesk COM+ application under component services must be set to the domain administrator. This is described in the next section.
- The core.asp file must be edited to include the second core. If this is a dual install, both core files under \inetpub\wwwroot\remote\xml and \inetpub\wwwroot\LANDesk\ldsm\xml must be edited.

### To log into a core in a multi-core environment

1. Launch Server Manager on one of the cores.
2. Select the core that you are actually opening Server Manager on from the drop-down menu. Type the user name and password.

### Notes

- To successfully complete client configuration, use the correct URL for the core. Otherwise, the configuration will not work.
- You may find it useful to add entries for each core server to your Favorites menu in Internet Explorer. This facilitates switching between cores.

## Configuring COM+ server credentials

When using a Web console server that isn't on the core, or if you want to use domain groups inside the LANDesk Management Suite group on the core server, there is some additional server configuration you must do for Management Suite authentication to work correctly. Remote Web console servers must get database connection information and user information from the core server, but since remote Web console servers use impersonated Web credentials on IIS, they can't communicate with the core server directly.

To solve this issue, the Web console server and core server use a COM+ application to communicate via HTTPS, allowing the Web console server to get core server database and user information. You need to configure this COM+ application on the Web console server to use an account that has the necessary rights, such as the domain administrator account. The account that you provide needs to be in the LANDesk Management Suite group on the core server (this allows it to access core server database connection information), and it needs to have rights to enumerate Windows domain members.

If you're using domain groups inside the core server's LANDesk Management Suite group, Management Suite also needs to be able to enumerate Windows domain members. In this case, you also need to provide an account for the core server's LANDesk COM+ application.



**To configure the LANDesk COM+ application on a core or remote Web console server**

1. Go to the Web server or core server you want to configure.
2. From the Windows Control Panel's Administrative Tools, double-click **Component Services**.
3. Click **Component Services | Computers | My Computer | COM+ Applications**.
4. From the **LANDesk** COM+ application's shortcut menu, click **Properties**.
5. On the **Identity** tab, enter the credentials you want to use.
6. Click **OK**.

# **Appendices, copyright, and build information**

---

## **Appendix A: System requirements and port usage**

The core must have a static IP address.

- [Administrative Core](#)
- [Server Support \(agents\)](#)
- [Browsers](#)
- [Databases](#)
- [Microsoft Data Access Components](#)
- [Port usage](#)

### **Administrative Core**

The administrative core supports the following operating systems:

- Microsoft Windows 2000 Server (with SP4)
- Microsoft Windows 2000 Advanced Server (with SP4)
- Microsoft Windows 2003 Server Standard Edition (with SP1)
- Microsoft Windows 2003 Server Enterprise Edition (with SP1)

### **Server Support (agents)**

- Microsoft Windows 2000 Server (with SP4)
- Microsoft Windows 2000 Advanced Server (with SP4)
- Microsoft Windows 2000 Professional (with SP4)
- Microsoft Windows 2003 Server Standard Edition (with SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (with SP1)
- Microsoft Windows 2003 Server Enterprise Edition (with SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (with SP1)
- Microsoft Windows XP Professional (with SP2)
- Windows Small Business Server 2000 (with SP4)
- Windows Small Business Server 2003 (with SP1)
- Red Hat Enterprise Linux v3 (ES)
- Red Hat Enterprise Linux v3 (ES) EM64t
- Red Hat Enterprise Linux v3 WS
- Red Hat Enterprise Linux v3 WS EM64t
- Red Hat Enterprise Linux v3 (AS)
- Red Hat Enterprise Linux v3 (AS) EM64t
- SUSE\* Linux Server 9
- SUSE Linux Enterprise Server 9 EM64t
- HP-UX 11.1
- Unix AIX

### **Browsers**

- Microsoft Internet Explorer 6.x (with SP1)

- Mozilla 1.7 and later
- Firefox 1.0.0 and later

## Databases

- MSDE (with SP4)
- MSSQL Server 2000 (with SP4)
- Oracle 8i (with 8.1.7)
- Oracle 9i (with 9.2.0.4)

## Microsoft Data Access Components

- MDAC 2.8 or later

If you want to have both LANDesk® Management Suite and Server Manager using the same database, you must install both products on the same "core" machine. Accordingly, if you want to install both products on the same "core" machine, you must use the same database. If both products use the same database, then LANDesk® Management Suite must also be version 8.6.

## Port usage

### Introduction

When using this product in an environment that includes firewalls (or routers that filter traffic), you may need to adjust firewall or router configurations to allow the product to operate. This section describes the ports used by the various product components. The information here focuses on information you need to configure routers and firewalls, leaving out ports only used locally (within individual subnets).

### Background information on firewall rules

This information applies to setting up firewall rules. If you aren't familiar with the subject, this section provides some generic background information on the main concepts.

### Firewall rules

"Opening a port" is not a precise term. You can't just go to a firewall and "open port x." Opening a port is shorthand for setting up a firewall rule. Firewall rules describe what traffic will or will not be allowed through the firewall. Firewall rules don't filter traffic on port number only. Rules can be based on protocols, source and destination port numbers, direction (inbound / outbound), source and destination IP addresses, and other things.

A typical firewall rule looks like this: "allow inbound traffic on TCP port 9535." For using this product, this rule is needed to support remote control. The rule is based on three elements:

1. The protocol (TCP or UDP)
2. The port number

### 3. The direction (inbound or outbound)

These three elements are required to set up firewall rules.

#### Source and destination ports, dynamic ports

There are always two ports involved in TCP or UDP communication. Any TCP or UDP packet is from a source port to a destination port. Firewall rules can be based on the source port, the destination port, or both. Ports listed in documents such as this one are always destination ports.

Well-known ports such as 5007 (used by the inventory service) refer to only one side of the communication. The other side of the communication is using a dynamic port. Dynamic ports are assigned automatically by the operating system in the range 1024-5000.

#### Firewalls and UDP traffic

To allow TCP traffic through a firewall, a single rule is sufficient, such as to allow inbound TCP connections to port 5007. Once the TCP connection is established, data can flow both ways through the connection.

UDP traffic is different because it is connectionless. For example, by default the core server will "ping" devices at UDP port 38293 before starting a task. A firewall rule that allows outgoing UDP packets to port 38293 will allow packets from the core server to a device outside the firewall, but not the device's response packets.

A rule that allows both outgoing and incoming packets to port 38293 won't work either because only one side of the communication is listening on the well-known port. The other side is using a dynamic port. Because the core server's outgoing packets are from a dynamic port to port 38293, the device's response packets are from port 38293 to the same dynamic port, not to port 38293. To allow two-way communication, a rule is needed that allows UDP packets with source port or destination port = 38293. Such a rule is usually acceptable on the intranet, but not on an external firewall (because it would allow inbound packets to all UDP ports).

For this reason, UDP traffic is usually not considered "firewall friendly". Coming back to the example, there is an alternative to UDP port 38293: TCP port 9595. When managing devices across a firewall, you probably want to configure the product to use the TCP port.

#### Ports used

Port	Direction	Protocol	Service
31770	console to device, device to core	TCP	communication between console and device
6787	console to device	TCP	communication between console and device

9595	console to device	UDP	discovery
623	console to device	UDP	ASF, IPMI discovery
9535	console to device	TCP	remote control

This product needs to discover nodes with the LANDesk agent installed before it can manage them. UDP port 9595 is used for discovery. You can also manually add individual devices to the console, but this still requires the device to respond to a "ping" on UDP port 9595. Communication between the console and the device uses TCP ports 31770 and 6787. Traffic on the latter port is HTTP-based. UDP port 623 is used for ASF (alert standard forum) discovery. In addition, this product uses TCP port 9535 for remote control. IPMI discovery is linked with ASF discovery and uses the same port (udp/623).

## Appendix B: Activating the core server

Before you can use the console, you must first activate your core server using the Core Server Activation utility. This is normally a one-time procedure that only needs to be repeated if you purchase additional licenses. Use the Core Server Activation utility to:

- Activate a new server for the first time.
- Update an existing core server or switch from a trial-use license to a full-use license.
- Activate a new server with a 45-day trial-use license.

Start the utility by clicking **Start | All Programs | LANDesk | Core Server Activation**. If your core server doesn't have an Internet connection, see [Manually activating a core or verifying the node count data](#) later in this section.

Each core server must have a unique authorized certificate. Multiple core servers can't share the same authorization certificate, though they can verify node counts to the same LANDesk account.

Periodically, the core server generates node count verification information in the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file is periodically sent to the LANDesk Software licensing server. This file is in XML format and is digitally signed and encrypted. Any manual changes to this file will invalidate the contents and the next usage report to the LANDesk Software licensing server.

The core communicates with the LANDesk Software licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require you to perform any manual steps.

---

The Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you manually launch the dial-up connection and run the activation utility, the utility can use the dial-up connection to report usage data.

If your core server doesn't have an Internet connection, you can verify and send the node count manually, as described later in this section.

---

## Activating a server with a LANDesk Software account

Before you can activate a new server with a full-use license, you must have an account set up with LANDesk Software that licenses you for the LANDesk Software products and number of nodes you purchased. You will need the account information (contact name and password) to activate your server. If you don't have this information, contact your LANDesk Software sales representative.

Don't change the core server's date or time between installing the product and activating the core. The activation will fail. You will have to uninstall and reinstall the product.

### To activate a server

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Enter the **Contact name** and **Password** you want the core to use.
3. Click **Activate**.

## Activating a server with a trial-use license

The 45-day trial-use license activates your server with the LANDesk Software licensing server. Once the 45-day evaluation period expires, you won't be able to log in to the core server, and it will stop accepting inventory scans, but you won't lose any existing data in the software or database. During or after the 45-day trial use license, you can rerun the Core Server Activation utility and switch to a full activation that uses a LANDesk Software account. If the trial-use license has expired, switching to a full-use license will reactivate the core.

### To activate a 45-day evaluation

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core for a 45-day evaluation**.
3. Click **Evaluate**.

## Updating an existing account

The update option sends usage information to the LANDesk Software licensing server. Usage data is sent automatically if you have an Internet connection, so you normally shouldn't need to use this option to send node count verification. You can also use this option to change core server associated with the LANDesk Software account the core server. This option can also change a core server from a trial-use license to a full-use license.

### To update an existing account

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Update this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use. If you enter a name and password that's different than the one used to originally activate the core, this switches the core to the new account.
4. Click **Update**.

## Manually activating a core or verifying the node count data

If the core server doesn't have an Internet connection, the Core Server Activation utility won't be able to send node count data. You'll see a message prompting you to send activation and node count verification data manually through e-mail. E-mail activation is a quick and simple process. When you see the manual activation message on the core, or if you use the Core Server Activation utility and see the manual activation message, follow these steps.

### To manually activate a core or verify the node count data

1. When the core prompts you to manually verify the node count data, it creates a data file called ACTIVATE.XML in the "\Program Files\LANDesk\Server Manager" folder. Attach this file to an e-mail message and send it to [licensing@LANDesk.com](mailto:licensing@LANDesk.com). The message subject and body don't matter.
2. LANDesk Software will process the message attachment and reply to the mail address you sent the message from. The LANDesk Software message provides instructions and a new attached authorization file.
3. Save the attached authorization file to the "\Program Files\LANDesk\Authorization Files" folder. The core server immediately processes the file and updates its activation status.

If the manual activation fails or the core can't process the attached activation file, the authorization file you copied is renamed with a .rejected extension and the utility logs an event with more details in the Windows Event Viewer's Application Log.

## Appendix C: Configuring services

You can use the Configure Server Manager services applet to configure the following services for any of your core servers and databases:

- [Selecting a core server and database](#)
- [Configuring the Inventory service](#)
- [Configuring duplicate device name handling](#)
- [Configuring duplicate device ID handling](#)
- [Configuring the scheduler service](#)
- [Configuring the custom jobs service](#)
- [Configuring the multicast service](#)
- [Configuring the OS deployment service](#)
- [Configuring the BMC password](#)
- [Configuring the Intel AMT password](#)

To launch the Configure Server Manager Services applet, on the core server, click **Start | Program Files | LANDesk | LANDesk Configure Services**.

Before configuring a service, use the **General** tab to specify the core server and database you want to configure the service for.

---

**Note:** Any service configuration changes you make for a core server and database will not take effect until you restart the service on that core server.

---

## Selecting a core server and database

The **General** tab lets you select a core server and database and provide authentication credentials so that you can configure services for that core server.

### About the Configure Server Manager services dialog: General tab

Use this dialog to select the core server and database you want to configure a specific service for. Then, select the service tab and specify the settings for that service.

- **Server name**—Displays the name of the core server you're currently connected to.
- **Server**—Lets you enter the name of a different core server and its database directory.
- **Database**—Lets you enter the name of the core database.
- **Username**—Identifies a user with authentication credentials to the core database (specified during Setup).
- **Password**—Identifies the user's password required to access the core database (specified during Setup).
- **This is an Oracle database**—Indicates that the core database specified above is an Oracle database.
- **Refresh settings**—Restores the settings that were present when you opened the Service Configuration dialog.

## Configuring the Inventory service

Use the **Inventory** tab to configure the Inventory service for the core server and database you selected using the General tab.

### About the Configure Server Manager services dialog: Inventory tab

Use this tab to specify the following inventory options:

- **Server name**—Displays the name of the core server you're currently connected to.
- **Log statistics**—Keeps a log of core database actions and statistics.
- **Scan server at**—Specifies the time to scan the core server.
- **Perform maintenance at**—Specifies the time to perform standard core database maintenance.
- **Days to keep inventory scans**—Sets the number of days before the inventory scan record is deleted.
- **Primary owner logins**—Sets the number of times the inventory scanner tracks logins to determine the primary owner of a device. The primary owner is the user who has logged in the most times within this specified number of logins. The default value is 5 and the minimum and maximum values are 1 and 16, respectively. If all of the logins are unique, the last user to log in is considered the primary owner. A device can have only one primary owner associated with it at a time. Primary user login data includes the user's fully qualified name in either ADS, NDS, domain name, or local name format (in that order), as well as the date of the last login.
- **Software**—Opens the **Software scanning** dialog where you can configure server software scanning time and history settings.



- **Device name**—Opens the Duplicate Devices dialog where you can choose an option to remove devices with duplicate device names, MAC addresses, or both.
- **Duplicate ID**—Opens the **Duplicate device ID** dialog where you can select attributes that uniquely identify devices. You can use this option to avoid having duplicate device IDs scanned into the core database (see Configuring duplicate device ID handling below).
- **Inventory service status**—Indicates whether the service is started or stopped on the core server.
- **Start**—Starts the service on the core server.
- **Stop**—Stops the service on the core server.

### About the Software scanning dialog

Use this dialog to configure the frequency of software scans. A device's hardware is scanned each time the inventory scanner is run on the device, but the device's software is scanned only at the interval you specify here.

- **Every login**—Scans all of the software installed on the device every time the user logs on.
- **Once every (days)**—Scans the device's software only on the specified daily interval, as an automatic scan.
- **Save history (days)**—Specifies how long the device's inventory history is saved.

### Configuring duplicate device name handling

Use the Duplicate Devices dialog to delete duplicate devices from the database.

1. In the Inventory tab, click **Device Name**.
2. In the Duplicate Devices dialog, click the option you want to use when deleting duplicate devices, then click **OK**.

#### Remove duplicate when:

- **Device names match:** Removes the older record when two or more device names in the database match.
- **MAC addresses match:** Removes the older record when two or more MAC addresses in the database match.
- **Both device names and MAC addresses match:** Removes the older record ONLY when two or more device names and MAC addresses (for the same record) match.

### Configuring duplicate device ID handling

Because imaging is often used to configure devices in a network, the possibility of duplicate device IDs among devices is increased. You can avoid this problem by specifying other device attributes that, combined with the device ID, create a unique identifier for your devices. Examples of these other attributes include device name, domain name, BIOS, bus, coprocessor, and so on.

The duplicate ID feature lets you select device attributes that can be used to uniquely identify the server. You specify what these attributes are and how many of them must be missed before the device is designated as a duplicate of another

device. If the inventory scanner detects a duplicate device, it writes an event in the applications event log to indicate the device ID of the duplicate device.

### To configure duplicate ID handling

1. In the Configure services dialog, click the **Inventory** tab, then click **Device ID**.
2. Select attributes from the Attributes list that you want to use to uniquely identify a device, and then click the right-arrow button to add the attribute to the Identity Attributes list. You can add as many attributes as you like.
3. Select the number of identity attributes (and hardware attributes) that a device must fail to match before it's designated as a duplicate of another device.
4. If you want the inventory scanner to reject duplicate device IDs, check the **Reject duplicate identities** option.

### About the Duplicate device ID dialog

Use this dialog to configure duplicate device ID handling.

- **Attributes list**—Lists all of the attributes you can choose from to uniquely identify a device.
- **Identity attributes**—Displays the attributes you've selected to uniquely identify a device.
- **Duplicate device ID triggers**—
  - **Identity attributes**—Identifies the number of attributes that a device must fail to match before it's designated as a duplicate of another device.
  - **Hardware attributes**—Identifies the number of hardware attributes that a device must fail to match before it's designated as a duplicate of another device.
- **Reject duplicate identities**—Causes the inventory scanner to record the device ID of the duplicate device and reject any subsequent attempts to scan that device ID. Then, the inventory scanner generates a new device ID.

## Configuring the scheduler service

Use the **Scheduler** tab to configure the scheduler service for the core server and database you selected using the General tab.

You must have the appropriate rights to perform these tasks, including full administrator privileges to the managed devices, allowing them to receive package distributions from Server Manager. You can specify multiple login credentials to use on devices by clicking **Change login**.

### About the Configure Server Manager services dialog: Scheduler tab

Use this tab to see the name of the core server and the database that you selected earlier, and to specify the following scheduled task options:

- **Username**—The username under which the scheduled tasks service will be run. This can be changed by clicking the **Change login** button.

- **Number of seconds between retries**—When a scheduled task is configured with multiple retries, this setting controls the number of seconds the Scheduled Tasks will wait before retrying the task.
- **Number of seconds to attempt wake up**—When a scheduled task is configured to use Wake On LAN, this setting controls the number of seconds that the scheduled tasks service will wait for a device to wake up.
- **Interval between query evaluations**—A number that indicates the amount of time between query evaluations, and a unit of measure for the number (minutes, hours, days, or weeks).
- **Wake on LAN settings**—The IP port that will be used by the Wake On LAN packet set by the scheduled tasks to wake up devices.
- **Schedule service status**—Indicates whether the service is started or stopped on the core server.
- **Start**—Starts the service on the core server.
- **Stop**—Stops the service on the core server.

### About the Configure Server Manager services dialog: Change login dialog

Use the **Change login** dialog (click **Change login** on the **Scheduler** tab) to change the default scheduler login. You can also specify alternate credentials the scheduler service should try when it needs to execute a task on unmanaged devices.

To install Server Manager agents on unmanaged devices, the scheduler service needs to be able to connect to devices with an administrative account. The default account the scheduler service uses is LocalSystem. The LocalSystem credentials generally work for devices that aren't in a domain. If devices are in a domain, you must specify a domain administrator account.

If you want to change the scheduler service login credentials, you can specify a different domain-level administrative account to use on devices. If you're managing devices across multiple domains, you can add additional credentials the scheduler service can try. If you want to use an account other than LocalSystem for the scheduler service, or if you want to provide alternate credentials, you must specify a primary scheduler service login that has core server administrative rights. Alternate credentials don't require core server administrative rights, but they must have administrative rights on devices.

The scheduler service will try the default credentials and then use each credential you've specified in the **Alternate credentials** list until it's successful or runs out of credentials to try. Credentials you specify are securely encrypted and stored in the core server's registry.

You can set these options for the default scheduler credentials:

- **Username**—Enter the default domain\username or username you want the scheduler to use.
- **Password**—Enter the password for the credentials you specified.
- **Confirm password**—Retype the password to confirm it.

You can set these options for additional scheduler credentials:

- **Add**—Click to add the username and password you specified to the Alternate Credentials list.
- **Remove**—Click to remove the selected credentials from the list.
- **Modify**—Click to change the selected credentials.

When adding alternate credentials, specify the following:

- **Username**—Enter the username you want the scheduler to use.
- **Domain**—Enter the domain for the username you specified.
- **Password**—Enter the password for the credentials you specified.
- **Confirm password**—Retype the password to confirm it.

## Configuring the custom jobs service

Use the **Custom jobs** tab to configure the custom jobs service for the core server and database you selected using the General tab. Examples of custom jobs include inventory scans or software distributions.

When you disable TCP remote execute as the remote execute protocol, custom jobs uses the Standard LANDesk agent protocol by default, whether it's marked disabled or not. Also, if both TCP remote execute and Standard LANDesk agent are enabled, custom jobs tries to use TCP remote execute first, and if it's not present, uses Standard LANDesk remote execute.

The **Custom jobs** tab also enables you to choose options for server discovery. Before the custom jobs service can process a job, it needs to discover each server's current IP address. This tab allows you to configure how the service contacts servers.

### About the Configure Server Manager services dialog: Custom jobs tab

Use this tab to set the following custom jobs options:

#### Remote execute options:

- **Disable TCP execute**—Disables TCP as the remote execute protocol, and thereby uses the CBA protocol by default.
- **Disable CBA execute / file transfer**—Disables the Standard Server Manager agent as the remote execute protocol. If Standard Server Manager agent is disabled and TCP remote execute protocol is not found on the device, the remote execution will fail.
- **Enable remote execute timeout**—Enables a remote execute timeout and specifies the number of seconds after which the timeout will occur. Remote execute timeouts trigger when the device is sending heartbeats, but the job on the device is hung or in a loop. This setting applies to both protocols (TCP or Standard Server Manager agent). This value can be between 300 seconds (5 minutes) and 86400 seconds (1 day).
- **Enable client timeout**—Enables a device timeout and specifies the number of seconds after which the timeout will occur. By default, TCP remote execute sends a heartbeat from device to device in intervals of 45 seconds until the remote execute completes or times out. Client timeouts are triggered when the device doesn't send a heartbeat to the device.
- **Remote execute port (default is 12174)**—The port over which the TCP remote execute occurs. If this port is changed, it must also be changed in the client configuration.

#### Distribution options:

- **Distribute to <nn> servers simultaneously**—The maximum number of devices to which the custom job will be distributed simultaneously.

**Discovery options:**

- **UDP**—Selecting UDP uses a standard Server Manager agent ping via UDP. Most Server Manager components depend on the Standard Server Manager agent, so your managed devices should have the Standard Server Manager agent on them. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping **Retries** and **Timeout**.
- **TCP**—Selecting TCP uses an HTTP connection to the server on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both**—Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Disable subnet broadcast**—When selected, disables discovery via a subnet broadcast.
- **Disable DNS/WINS lookup**—When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

## Configuring the multicast service

Use the **Multicast** tab to configure the multicast domain representative discovery options for the core server and database you selected using the **General** tab.

### About the Configure Server Manager services dialog: Multicast tab

Use this tab to set the following multicast options:

- **Use multicast domain representative:** Uses the list of multicast domain representatives stored in the network view's **Configuration > Multicast domain representatives** group.
- **Use cached file:** Queries each multicast domain to find out who might already have the file cached. The cached file can then be used instead of downloading the file to a representative.
- **Use cached file before preferred domain representative:** Changes the order of discovery to make **Use cached file** the first option attempted.
- **Use broadcast:** Sends a subnet-directed broadcast to find any device in that subnet that could be a multicast domain representative.
- **Log discard period (days):** Specifies the number of days that entries in the log will be retained before being deleted.

## Configuring the OS deployment service

Use the **OS deployment** tab to designate PXE representatives as PXE holding queues, and to configure basic PXE boot options for the core server and database you selected using the **General** tab.

PXE holding queues are one method of deploying OS images to PXE-enabled devices. You designate existing PXE representatives (located in the **Configuration** group in the network view) as PXE holding queues. For more information, see "[PXE-based deployment](#)."

Select and move PXE representatives from the **Available proxies** list to the **Holding queue proxies** list.

## About the Configure Server Manager services dialog: OS deployment tab

Use this tab to assign PXE holding queue proxies (representatives), and to specify the PXE boot options.

- **Available proxies:** Lists all available PXE proxies on your network, identified by device name. This list is generated when the inventory scanner detects PXE software (PXE and MTFTP protocols) running on the device.
- **Holding queue proxies:** Lists the PXE proxies that have been moved from the **Available proxies** list, thereby designating the proxy as a PXE holding queue. PXE-enabled devices on the same subnet as the PXE holding queue proxy will be automatically added to the **PXE holding queue** group in the console's network view when they PXE boot. The devices can then be scheduled for an image deployment job.
- **Reset:** Forces all of the PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the **PXE holding queue** group in the console's network view. The devices can then be scheduled for an imaging job. (The Reset button is enabled when you select a PXE proxy in the Holding queue proxies list.)
- **PXE boot options:** Determines how the PXE boot prompt operates when devices attempt to PXE boot.

**Note:** Changes you make here to the PXE boot options will not take effect on any of your PXE representatives until you run the PXE Representative Deployment script on that representative.

- **Timeout:** Indicates how long the boot prompt displays before timing out and resuming the default boot process. The maximum number of seconds you can enter is 60 seconds.
- **Message:** Specifies the PXE boot prompt message that appears on the device. You can type any message you like in the text box, up to 75 characters in length.

## Configuring the BMC password

Use the **BMC password** tab to create a password for the IPMI Baseboard Management Controller (BMC).

1. In the **BMC password** tab, type a password in the **Password** text box, retype the password in the **Confirm password** text box, then click **OK**.

The password cannot be longer than 15 characters, each of which must be numbers 0-9 or upper/lower case letters a-z.

## Configuring the Intel AMT password

Use the **Intel AMT password** tab to create or change the password on an Intel Active Management Technology-enabled device.

1. In the **Intel AMT Password** tab, type the current AMT password and confirm it. This authenticates you to the device.
2. Type the new AMT password and confirm it.

**Note:** The new password must be a strong password, meaning that the password

- Is at least seven characters long
- Contains letters, numbers and symbols
- Has at least one symbol character in the second through sixth positions
- Is significantly different from prior passwords
- Doesn't contain names or user names
- Isn't a common word or name

## Appendix D: Agent security and trusted certificates

Each core server has a unique certificate and private key that Setup creates when you first install the core server on a device. Devices will only communicate with core servers for which they have a matching trusted certificate file.

These are the private key and certificate files that are installed:

- **<keyname>.key**—The .KEY file is the private key for the core server, and it only resides on the core server. If this key is compromised, the core server and server communications won't be secure. Keep this key secure. For example, don't use e-mail to move it around.
- **<keyname>.crt**—The .CRT file contains the public key for the core server. The .CRT file is a viewer-friendly version of the public key that you can view to see more information about the key.
- **<hash>.0**—The .0 file is a trusted certificate file and has content identical to the .CRT file. However, it's named so that the computer can quickly find the certificate file in a directory that contains many different certificates. The name is a hash (checksum) of the certificate's subject information. To determine the hash filename for a particular certificate, view the <keyname>.CRT file. There is a .INI file section [LDMS] in the file. The hash=value pair indicates the <hash> value.

All keys are stored on the core server in \Program Files\LANDesk\Shared Files\Keys. The <hash>.0 public key is also in the LDLOGON directory and needs to be there by default. <Keyname> is the certificate name you provided during core server setup. During setup, it's helpful to provide a descriptive key name, such as the core server's name (or even its fully qualified name) as the key name (example: Idcore or Idcore.org.com). This will make it easier to identify the certificate/private key files in a multi-core environment.

## Backing up and restoring certificate/private key files among core servers

When you install a core server, Setup creates a new certificate. If you reinstall over an existing core server, Setup still creates a new certificate. If you install devices with a certificate that doesn't match your new core server certificate, the core server won't be able to communicate with them. If you need to reinstall your core server, you have two options:

1. Reinstall the agents manually with a configuration built on your new core server. You can't use software distribution to update the agents, because the core server and devices don't have a matching certificate and key.



2. Before reinstalling a core server, back up the existing certificate and key files to a safe place. After you have reinstalled, copy the old keys to the new core installation. The new and old keys can coexist. The core will use the appropriate key automatically.

Cores can contain multiple certificate/private key files. As long as a client can authenticate with one of the keys on a core, it can communicate with that core.

A utility is included in this product that performs the second option listed above. The core data migration utility (CoreDataMigration.exe) is installed in the \ProgramFiles\LANDesk\ManagementSuite folder. It handles the backing up and copying of data such as keys and certificates when you install a new core.

#### **To save and restore a certificate/private key set**

1. At the source core server, go to the \Program Files\LANDesk\Shared Files\Keys folder.
2. Copy the source server's <keyname>.key, <keyname>.crt, and <hash>.0 files to a floppy disk or other secure place.
3. At the destination core server, copy the files from the source core server to the same folder (\Program Files\LANDesk\Shared Files\Keys). The keys take effect immediately.

---

#### **Warning: Keep the private key file secure**

Make sure that the private key <keyname>.key isn't compromised. Don't transfer it using an insecure method, like e-mail or a public file share. The core server uses this file to authenticate devices, and any core with the appropriate <keyname>.key file can perform remote executions and file transfer to a managed device.

---

## **Appendix E: Additional OS deployment procedures**

The chapter provides supplemental information about LANDesk's OS imaging capabilities.

Read this chapter to learn about:

- [Adding application package distributions to the end of an OSD script](#)
- [Using CSVIMPORT.EXE to import inventory data](#)
- [Creating custom computer names](#)
- [Customizing the SYSPREP.INF \[RunOnce\] section with tokenized inventory values](#)
- [Using images in mixed uniprocessor and multiprocessor environments](#)
- [Using the LANDesk imaging tool for DOS](#)
- [Using the LANDesk imaging tool for Windows](#)



## Additional OS deployment procedures

### Adding application package distributions to the end of an OSD script

You can easily make an Software Distribution (SWD) application package distribution part of your OS deployment script.

#### To add SWD packages to an OS deployment script

1. Open your package script in the LANDesk/ManagementSuite/Scripts directory and copy the REMEXECx= package distribution lines.
2. Edit your script by right-clicking it in the **Scripts** window and clicking **Edit**.
3. Paste the ESW REMEXEC commands at the bottom of your script, changing the REMEXEC numbering so that the numbers are sequential.
4. Insert a line before the SWD lines you pasted in for LDSLEEP, similar to below. This allows time for the OS to finish booting before starting the package installation.

```
REMESECxx=LDSLEEP.EXE 120
```

Replace xx with a unique sequential number.

### Using CSVIMPORT.EXE to import inventory data

You can use a command-line utility that allows you to import inventory data into the core database. This can be useful if you're installing new devices and you have information like MAC addresses available. You can use CSVIMPORT.EXE to import this data to the product so you can target devices ahead of time for OS deployment jobs.

CSVIMPORT.EXE requires a template file describing the field contents and what columns in the core database the data should go in. CSVIMPORT.EXE also requires the .CSV file containing the data matching the template file you specify. CSVIMPORT.EXE creates miniscan files that you can then copy to the LANDesk/ManagementSuite/LDScan directory so they get added to the core database.

#### Sample template file:

```
Network - NIC Address = %1%
Network - TCP/IP - Adapter 0 - Subnet Mask = 255.255.255.0
BIOS - Serial Number = %2%
BIOS - Asset Tag = %3%
Display Name = %4%
```

Note that you can include custom data in the files. The entries %1, %2, and so on refer to the first, second, and so on columns. The subnet mask in this case will be applied to all entries as 255.255.255.0. The template file can't have any header text other than the actual template information.

**Sample .CSV file:**

```
0010A4F77BC3, SERIAL11, ASSETTAG-123-1, MACHINE1
0010A4F77BC4, SERIAL21, ASSETTAG-123-2, MACHINE2
0010A4F77BC5, SERIAL31, ASSETTAG-123-3, MACHINE3
0010A4F77BC6, SERIAL41, ASSETTAG-123-4, MACHINE4
0010A4F77BC7, SERIAL51, ASSETTAG-123-5, MACHINE5
0010A4F77BC8, SERIAL61, ASSETTAG-123-6, MACHINE6
```

Run CSVIMPORT with these three parameters: <templateFilename> <csvFileName> <outputDirectoryForScanFiles>. If you want the output to be entered in the core database immediately, specify your LANDesk/ManagementSuite/LDScan directory for output.

## Creating custom computer names

The **Assign naming convention for target computers** page of the OS Deployment wizard lets you create computer names based on MAC addresses, text you enter, and counters (nnn...). You can also create names based on inventory data for asset tags, serial numbers, and login names by creating a COMPUTERNAME.INI file in your Management Suite directory.

**COMPUTERNAME.INI syntax:**

```
[Rename Operations]
tok0=ASSET TAG
tok1=SERIAL NUMBER
tok2=LOGIN NAME
```

The values returned by the .INI file substitute for the \$MAC token in the wizard's naming convention page.

You can only use the above three inventory values in the file. OS deployment checks the options in the numeric tok<x> order. All three of the above tokens don't have to be in the file. The first tok<x> option found that has an equivalent database entry substitutes for the \$MAC token for the device being imaged. For example, in the case above, if there were no asset tag or serial number entries in the database, but there was a login name, the login name would be used for the \$MAC token. If none of the options match, the MAC address is used for the \$MAC token.

The login name option returns the login name returned by the most recent inventory scan.

## Using the nnn computer name token

The **Assign naming convention for target computers** page of the OS Deployment wizard includes an nnn option that substitutes for a 3-15 digit number, depending on how many n characters you specify. For each computer name template you use in the wizard, OS deployment keeps a running counter of the numbers used. This way, subsequent jobs continue where the last job left off.

Every unique template has its own counter. If you always use the same template, the counter will span jobs. If you change your template after deploying some devices

and later decide to go back to the template you originally used, the counter remembers where you left off for that template and continues counting.

## Customizing the SYSPREP.INF [RunOnce] section with tokenized inventory values

The SYSPREP.INF contains a [RunOnce] section that specifies programs to run after the device boots for the first time. If you add your own programs to that section, you can include database tokens on the program command line if they're useful to the program you're running. OS deployment substitutes the token you specify with corresponding information from the core database.

### Sample tokens:

%Computer - Device Name%  
 %Computer - Login Name%  
 %Computer - Manufacturer%  
 %Computer - Model%  
 %Computer - Type%  
 %Computer - BIOS - Asset Tag%  
 %Computer - BIOS - Service Tag%  
 %Network - TCPIP - Address%  
 %System - Manufacturer%  
 %System - Model%  
 %System - Serial Number%  
 %Processor - Processor Count%  
 %Computer - Workgroup%  
 %Computer - Domain Name%

You can chain multiple tokens together. For example, to separate two tokens by a colon: %Computer - Workgroup%:%Computer - Device Name% could return MyWorkgroup:MyComputer.

---

**Note:** You should only use tokens that return a single value.

---

## Using images in mixed uniprocessor and multiprocessor environments

Uniprocessor and multiprocessor devices require different Windows 2000 and Windows XP images. Depending on your hardware configuration, you may be able to use your uniprocessor image on a multiprocessor device, or vice versa.

Devices that support advanced processor features typically have an Advanced Programmable Interrupt Controller (APIC). Devices that support advanced processor features can also have an Advanced Configuration and Power Interface (ACPI).

---

**Note:** The support matrix for sharing an image between uniprocessor and multiprocessor devices is complex. You should refer to Microsoft's UNATTEND.TXT file for more details. Generally, you need to remember the following when sharing uniprocessor and multiprocessor images: **Both the source and target devices must have either an ACPI APIC HAL or a non-ACPI APIC HAL. You can't use an ACPI APIC image on a non-ACPI APIC device, or vice versa.**

---

**To configure multiple processor information**

1. In the Configure multiprocessor information page of the OS Deployment wizard, click **Configure advanced multiprocessor options**.
2. Select whether you're deploying a **Windows 2000**, **Windows 2003**, or a **Windows XP** image.
3. Select whether the image you're using was created on a **Uniprocessor** or **Multiprocessor** device.
4. Your source and target devices have the same HAL. If your image was created on an APIC ACPI device, select **APIC**. If your image was created on a non-ACPI APIC device, select **MPS**.

## Using the LANDesk imaging tool for DOS

---

**Note:** When you install the OS deployment component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT, and BACKALL.BAT.

---

LANDesk's imaging tool for DOS (IMAGE.EXE) is a DOS-based backup and restore utility that creates a snapshot of an entire partition or volume and saves it to a set of files, or saves it directly to most ATAPI CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

**Limitations**

IMAGE.EXE relies on the BIOS for processing disk functions. If a computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGE.EXE will also be limited.

**System requirements**

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- 16 MB RAM
- XMS

**Getting started**

IMAGE.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

**Environment variables**

You can use several different environment variables with IMAGE.EXE:

- **IMSG** displays a message on the screen. To create a message with IMSG, use the set command (i.e., set img=<include message of 80 characters or less here>).
- **IBXT** changes the method used to burn a set of CDs so that IMAGE.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1. (i.e., set ibxt=1). This setting may not work with all CD-R/RW drives.

- **IAR** enables IMAGE.EXE to auto-respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set iar=Y). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.
- **IOBS=A** tests the network speed and uses the best buffer size for uploading/downloading an image.

### Command-line options

You can use command-line options with IMAGE.EXE. Separate the options by spaces and enter them in the order shown below. Use the /? command-line option to view a list of additional command-line options not explained here.

#### To create a compressed image to a file

Format 1: image /Ch# d:\filename.img (no validation)

Format 2: image /Ch#V d:\filename.img (validation)

Format 3: image /Ch#VB d:\filename.img (byte-for-byte validation)

Explanation: Replace the h with the source hard drive number from 0 to 7 and the # with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as 0xPVV where P is the extended partition and VV is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGE.EXE without any command-line options and select Create Image. The screen that lists the partitions and volumes will display the ID in parentheses as a hexadecimal number. You should prefix that number with a 0x on the command line.

#### To create an uncompressed image to a file

Format 1: image /Ch# /U d:\filename.img (no validation)

Format 2: image /Ch#V /U d:\filename.img (validation)

Format 3: image /Ch#VB /U d:\filename.img (byte-for-byte validation)

Explanation: Same as above.

#### To create a compressed image to a CD drive

Format 1: image /Ch# /CDx (ATAPI)

Format 2: image /Ch# /CDSx (ASPI)

Explanation: The h and # information is the same as above. The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS) to get a list of the devices.

#### To create an uncompressed image to a CD drive

Format 1: image /Ch# /U /CDx (ATAPI)

Format 2: image /Ch# /U /CDSx (ASPI)

Explanation: Same as above.

**To restore an image from a file**

Format 1: image /R d:\filename.img (no validation)

Format 2: image /RV d:\filename.img (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

**To restore an image from a CD**

Format 1: image /R /CDx (ATAPI)

Format 2: image /R /CDSx (ASPI)

Explanation: The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS) to get a list of the devices.

**To limit the file size on creation**

Format: d:\filename;s

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.

**Issues to be aware of**

- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- When restoring an image, you shouldn't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system will reboot. This is required because the partitions and file system being used by the OS have changed. If a reboot didn't occur, the OS would still think the partition and file system was as it was before the restore. This could cause data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition goes to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If an existing partition or volume occupies the same starting location as the partition to be restored, then a warning message is issued before overwriting that partition or volume.
- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGE.EXE via AUTOEXEC.BAT if desired.

## Using the LANDesk imaging tool for Windows

LANDesk's imaging tool for Windows (IMAGEW.EXE) is a Windows 32-based backup and restore utility that creates a snapshot of an entire partition or volume and saves

it to a set of files, or saves it directly to most types of DVD+RW or CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

IMAGEW.EXE is compatible with LANDesk's imaging tool for DOS (IMAGE.EXE).

### Limitations

For use with Windows 9x/Me, IMAGEW.EXE requires that the system support Int 13h extensions. If your computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGEW.EXE will also be limited on those OSes.

### System requirements

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- Windows 32-based environment with 32 MB RAM minimum recommended
- Administrator privileges when running on Windows NT, Windows 2000, or Windows XP

IMAGEW.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

### Creating images

You can use various environment variables and command-line options to ensure that the images you create meet your requirements.

### Environment variables

Environment variables for IMAGEW.EXE must be used with command-line options. The following environment variables are available:

- **IBXT** changes the method used to burn a set of CDs so that IMAGEW.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1 (i.e., set ibxt=1). This setting may not work with all CD-R/RW drives.
- **IAR** enables IMAGEW.EXE to auto respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set iar=Y). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.

### Command-line options

You can use command-line options with IMAGEW.EXE. Separate the options by spaces and enter them in the order shown below. Use the /? command-line option for additional command-line options not explained here.

### To create a compressed image to a file

Format 1: `imagew /Ch# d:\filename.img` (no validation)

Format 2: `imagew /Ch#V d:\filename.img` (validation)

Format 3: `imagew /Ch#VB d:\filename.img` (byte-for-byte validation)

Explanation: Replace the h with the source hard drive number from 0 to 7 and the # with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as 0xPVV where P is the extended partition and VV is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGEW.EXE without command-line options and select Create Image. The screen that lists the partitions and volumes will also display the ID in parentheses as a hexadecimal number. You should prefix that number with a 0x on the command line.

#### **To create an uncompressed image to a file**

Format 1: `imagew /Ch# /U d:\filename.img` (no validation)

Format 2: `imagew /Ch#V /U d:\filename.img` (validation)

Format 3: `imagew /Ch#VB /U d:\filename.img` (byte-for-byte validation)

Explanation: Same as above.

#### **To create a compressed image to a CD drive**

Format 1: `imagew /Ch# /CDx`

Explanation: The h and # information is the same as above. The x after /CD is the CD drive number to use. Omit the x (/CD) to get a list of the devices.

#### **To create an uncompressed image to a CD drive**

Format 1: `imagew /Ch# /U /CDx`

Explanation: Same as above.

#### **To restore an image from a file**

Format 1: `imagew /R d:\filename.img` (no validation)

Format 2: `imagew /RV d:\filename.img` (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

#### **To restore an image from a CD**

Format 1: `imagew /R /CDx`

Explanation: The x after /CD is the CD drive number to use. Omit the x to get a list of the devices.

#### **To limit the file size on creation**

Format: `d:\filename;s`

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.



**Issues to be aware of**

- When running under Windows NT/2000/XP Pro, you must have administrator privileges. Under Windows 2000/XP, you can run as any user by right-clicking and selecting the Run As option.
- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- If you create a backup without a lock being obtained, that backup may not be in a consistent state if updates to the drive were occurring during the backup.
- When restoring an image, you can't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system may need to reboot. This is required under certain conditions and determined by the program. If you don't reboot when asked, the OS will think the partition and file system is as it was before the restore, potentially causing data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition will go to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If an existing partition or volume occupies the same starting location as the partition to be restored, a warning message is issued before overwriting that partition or volume.
- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGEW.EXE via AUTOEXEC.BAT if desired.

## Appendix F: IPMI support

Server Manager includes support for Intelligent Platform Management Interface (IPMI) 1.5 and 2.0. IPMI is a specification developed by Intel,\* H-P,\* NEC,\* and Dell\* to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that let you access many features regardless of whether or not the machine is turned on, or what state the OS may be in. For more details on IPMI, visit Intel's Web site.

IPMI monitoring is based on the BMC (baseboard management controller). The BMC operates on standby power and autonomously polls system health status. If the BMC detects that any elements are out of range, you can configure the resulting IPMI actions, such as logging the event, generating alerts, or performing automatic recovery actions such as system power-down or reset.

You must have SMBIOS 2.3.1 or higher installed in order for the BMC to be detected on the system. If the BMC is not detected, you may not see some IPMI information in reports, exports, and so forth.

IPMI defines common interfaces to the hardware used to monitor physical health characteristics, such as temperature, voltage, fans, power supplies, and chassis intrusion. In addition to health monitoring, IPMI includes other system management

capabilities including automatic alerting, automatic system shutdown and restart, remote restart and power control capabilities, and asset tracking.

The Server Manager menu choices vary slightly for an IPMI-enabled device, depending on the state of the operating system.

## Management features for IPMI-enabled devices

Monitoring capabilities depend on what has been installed on the device being monitored, as well as the state of the device. Any IPMI-enabled device with a baseboard management controller (BMC) can be monitored by the administrator console in limited ways with no additional agency after the BMC has been configured. This includes out-of-band management when the device is powered down or the OS isn't functional. Full-featured management is available when the Server Manager monitoring agent is installed, a BMC is present, the device is powered on, and the OS is functional. The table below compares the functionality available with these different configurations.

	BMC only*	BMC + agent	Agent (no IPMI)
Out-of-band management enabled	X	X	
In-band management enabled		X	X
Device can be discovered**	X	X	X
Read environment sensors	X	X	Hardware dependent
Power on/off remotely	X	X	X
Read & clear event log	X	X	
Configure alerts	X	X	X
Read OS information		X	X
Graceful shutdown		X	X
Read SMBIOS information (processor, slots, memory)		X	X
IP syncing (OS to BMC)		X	
Watchdog timer		X	
BMC communicates with core server	X	X	
Local Server Manager components communicate with core server		X	X
Full range of Server Manager management features		X	

\*Standard BMC. The mini BMC is a scaled-down version of a baseboard management controller. It has the functionality listed above, with limitations such as the following:

- Does not support serial over LAN (SOL) redirection
- Has only one username for BMC management
- Uses only one channel for communicating with the BMC
- Has a smaller system event log (SEL) repository

\*\*If the BMC is not configured, it will not respond to ASF pings which the product uses to discover IPMI. This means that you will have to discover it as a normal computer. When you push the client, ServerConfig will scan the system and detect it is IPMI and configure the BMC.

## Appendix G: Intel® AMT support

Server Manager supports devices using Intel® Active Management Technology (Intel® AMT), a hardware and firmware functionality that enables remote device management. AMT uses out-of-band (OOB) communication for access to devices regardless of the state of the operating system or power to the device.

When devices are configured with Intel AMT, a limited number of management features are available even if the device does not have a Server Manager agent installed. As long as devices are connected to the network and have standby power, they can be discovered and can be added to inventory to be managed with other devices on the network.

If a device has AMT but no Server Manager agent installed, it can be discovered with unmanaged device discovery, moved to the inventory database, then viewed in the **My devices** list. However, many Server Manager management options are unavailable. These options are only made available when the Server Manager agent is installed. Management features that are available for AMT-configured devices include:

- **Inventory summary:** a subset of the normal inventory data can be queried and viewed in real time for the device even if the device is powered off.
- **Event log:** a log with AMT-specific events, showing severity and description of the events, can be viewed in real time.
- **Remote boot manager:** power cycling and several boot options can be initiated from the remote management console, regardless of the state of the device's OS or power. The options available are based on the support for the options on the device. Some devices may not support all boot options.
- **Force vulnerability scan and disable OS network:** if a device appears to have malicious software running, a vulnerability scan can be run at the next reboot; if necessary, the device's OS-level network access can be disabled to prevent unwanted packets from being spread on the network.

## Intel AMT provisioning requirements

In order to discover and manage devices with Intel AMT capabilities, each device must have been provisioned in Small Business mode. Server Manager does not support Enterprise mode (with TLS enabled) at this time. If the manufacturer did not

provision the device in Small Business mode, use the Intel AMT Configuration Screen to provision the device correctly (see the documentation provided by Intel for this Configuration Screen).

In order for the core server to authenticate with discovered Intel AMT devices, the AMT username/password credentials must match the credentials that you configure using the LANDesk Configure Services application. You can change the credentials using the Intel AMT Configuration Screen. You can also use LANDesk Configure Services to change the credentials (see To configure the Intel AMT password).

## Troubleshooting tips

The following troubleshooting tips are for issues that most frequently occur with the console.

### **I can't activate the core.**

If you installed a core, then changed the device time, you will not be able to activate. You must reinstall the product in order to activate the core.

### **I don't know the URL to the console pages.**

Contact the person who installed the core server, most likely the network administrator for your site. However, typically the URL is `http://core server machine name/ldsm`.

### **Who am I logged in as?**

Look above the bar below the name LANDesk Server Manager, at the **Connected As** section.

### **What machine am I logged in to?**

Look above the bar below the name LANDesk Server Manager, at the **Connected To** section.

### **I launch Server Manager, and I get a "Session Timed Out" message immediately.**

If you open Server Manager from the Favorites or Bookmark menu with the `/FRAMESET.ASPX` extension at the end of the URL, Server Manager will not launch correctly. To fix this, edit your Bookmarks or Favorites link to remove this extension, or paste the URL (without the extension) directly into the browser window.

### **If you don't see some of the left navigation pane links**

It's because your network administrator is most likely using LANDesk Server Manager's role-based administration or feature-level security option that limits you to performing certain tasks that you have the rights to do.

### **The scanner can't connect to the device.**

If the scanner can't connect to the device, verify that the Web application directory is configured correctly. If you're using https, you must have a valid certificate. Verify that you have a valid certificate.

### **I get a permission denied error when I try to access the console**

To use feature-level security on Windows 2000 and 2003, you must disable anonymous authentication. Verify the authentication settings on the Web site and the `..\LANDesk\ldsm` folder under the Web site.

1. On the server that hosts the Web console, click **Start | Administrative Tools | Internet Information Services (IIS) Manager**.
2. From the **Default Web Site** shortcut menu, click **Properties**.
3. On the **Directory Security** tab, in the **Anonymous access and authentication control** area, click **Edit**. Clear the **Enable anonymous access** option and check **Integrated Windows authentication** option.
4. Click **OK** to exit the dialogs.
5. From the Default Web Site's .\LANDesk\ldsm subfolder, click **Properties**. Repeat steps 3-4.

### **I get an invalid session when viewing the console.**

It's possible the browser session has timed out. Use your browser's **Refresh** button to start a new session.

### **The number of items per page is different from the number I specified.**

When you specify how many items to display per page, that setting is stored in the Web browser's cookies directory and expires when the console session times out.

### **The console times out too frequently.**

You can change the default session timeout for the console's Web pages. The IIS default is 20 minutes of inactivity before a login expires. To change the IIS session timeout:

1. On the Web server, open the IIS Internet Service Manager.
2. Expand the default Web site.
3. Right-click the **LDSM** folder, then click **Properties**.
4. Under the **Virtual Directory** tab, click **Configuration**.
5. Click the **Application Options** tab, then change the session timeout to the value you want.

Note: LANDesk Server Manager 8.6 is a session-based product. Do not disable the session state.

### **I cannot view the Remote control page in the Web console.**

In order to view the Remote **control** page, you must enable ActiveX controls. Some browsers have ActiveX controls disabled by default. If the Remote **control** page does not load correctly, enable ActiveX controls on your browser by changing the security settings.

### **I completed the software distribution wizard, but the console did not create a package.**

The console uses the IUSR and IWAM accounts on console server. These accounts are originally created based on the computer name. If you have ever changed the computer name, you must follow the steps below in order to successfully create software distribution packages.

1. If you have .Net Framework installed, uninstall it.
2. Uninstall IIS.
3. Reinstall IIS.
4. Reinstall the .Net Framework if you uninstalled it.

### **A scheduled software distribution job did not run.**

If you schedule a software distribution job and it does not start, verify that the Intel Scheduler Service is running on the device.

Also, take into consideration that the scheduling of the job is based on the core server's time. If the job was scheduled on a console that resides in another time zone, the job will start based on the core server's time, which may be different than expected.

#### Report charts don't display properly.

In order to view the interactive bar and pie charts displayed in many reports, you must have Macromedia Flash Player\* 7 installed. Verify that Flash is installed, then run the report again.

#### Web console error about not being able to authenticate to the database.

If you use an Oracle 9.2.0.1, there is an Oracle install bug that doesn't set the proper permissions for authenticated users (which IIS uses). If you see a Web console error about not being able to authenticate to the database, follow these steps to fix it.

1. Log in to Windows as a user with administrator privileges.
2. Launch Windows Explorer from the **Start** menu and navigate to the ORACLE\_HOME folder. This is typically the Ora92 folder under the Oracle folder (i.e. D:\Oracle\Ora92).
3. From the ORACLE\_HOME folder's shortcut menu, click **Properties**.
4. Click the **Security** tab.
5. In the **Name** list, click **Authenticated Users**. On Windows XP, the Name list is called **Group or user names**.
6. In the **Permissions** list under the **Allow** column, clear the **Read and Execute** option. On Windows XP, the **Permissions** list is called **Permissions for Authenticated Users**.
7. Re-check the **Read and Execute** option under the **Allow** column (this is the box you just cleared).
8. Click **Advanced**, and in the **Permission Entries** list, make sure you see the **Authenticated Users** listed there with Permission = Read & Execute and Apply To = This folder, subfolders and files. If this isn't the case, edit that line and make sure the **Apply onto** box is set to **This folder, subfolders and files**. This should already be set properly, but it's important that you verify this.
9. Click the **OK** until you close out all of the security properties windows.
10. Reboot your server to make sure that these changes have taken effect.

#### Oracle error on installation

During installation, you may see the following message:

```
OraOLEDB.Oracle.1 provider is not registered on the local machine.
```

If this happens, it is likely to be a rights issue. You are probably connecting to the Oracle database using a 9i client, and pertains to a known Oracle issue. If you are sure you have already installed the OraOLEDB driver, then try the following:

1. In the Windows Explorer, go to the OraHome92 directory (by default, it is C:\oracle\ora92), right-click this folder and select **Properties, Security**, select **Authenticated Users**, uncheck then re-check the **Allow** box for "Read & Execute" permission, then click **Apply**.

2. Click the **Advanced** button, check the **Allow inheritable permissions from parent to propagate to this object** and **Reset permissions on all child objects and enable propagation of inheritable permissions** checkboxes. Click **Apply**, and choose **Yes** when prompted. When this process is over, you'll notice that the **Allow inheritable permissions from parent to propagate to this object** checkbox is checked.
3. In the Command Prompt window, type "iisreset".

At this point, you should be able to authenticate to the database and use your console.

### **Why am I seeing two instances of the same device in my database?**

Have you deleted a device from the core database and reinstalled it using UninstallWinClient.exe?

UninstallWinClient.exe is in the LDMain share, which is the main ManagementSuite program folder. Only administrators have access to this share. This program uninstalls Management Suite or Server Manager agents on any device it runs on. You can move it to any folder you want or add it to a login script. It's a Windows application that runs silently without displaying an interface. You may see two instances of the device in the database you just deleted. One of these instances would contain historical data only, while the other would contain data going forward. See the *Deployment Guide* for more information on UninstallWinClient.exe.

### **Using the previous database from LDSM 8.6 or LDMS 8.X on an LDMS/LDSM 8.6 re-installation**

If you have uninstalled a previous installation of LDMS 8.X or LDSM 8.6 using the MSDE database on the same machine, the MSDE database and the instance created are not uninstalled, meaning that you can use them again if you want to reinstall LDSM/LDMS 8.6 on the same machine. You can look in the registry for connection information needed to connect to this database during re-install:

Key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\Local

the following string values correspond to what need to be filled out in the "User-supplied Database Configuration" page:

Server <hostname\ldmsdata>

User <sa>

Database <lddb>

Password (this could be encoded, depending on the value of "PWD Encrypted")

### **When I try to discover an IPMI device, it is not listed in the IPMI folder in the Unmanaged devices page.**

IPMI devices must have a BMC (baseboard management controller) that is configured in order to be discovered as IPMI devices and to use full IPMI functionality. If the BMC is not configured, the device can be discovered as a computer. You can then add the device to the list of managed devices and run the Configure Services utility to configure the BMC password. The device's IPMI functionality will then be recognized by this product.

### **I cannot get the address of the core server when I choose PXE Boot Menu**

When trying to run PXE Representative Deployment on a target machine, rebooting the device, pressing F8 and choosing PXE Boot Menu, you get the message "HTGET:



Cannot get address for <core server>. Error: Unable to resolve name : <core server> into an address .ParseCoreAddressInof failure

This is because the client is trying to download files from the Core Server using HTTP. The client will use WINS to resolve the Core Server name to IP address. If unable to download the files from the Core Server, HTGET errors will be returned.

To resolve this issue, please read the article

<http://kb.LANDesk.com/al/12/4/article.asp?aid=2558&n=7&tab=search&bt=4&r=0.1898264&s=1>

**I added a S.M.A.R.T. drive on a server, but I don't see S.M.A.R.T. drive monitoring in the inventory list for that server.**

Hardware monitoring is dependent on the capabilities of the hardware installed on a device, as well as on the correct configuration of the hardware. If a hard drive with S.M.A.R.T. monitoring capabilities is installed on a device but S.M.A.R.T. detection is not enabled in the device's BIOS settings, or if the device's BIOS does not support S.M.A.R.T. drives, monitoring data will not be available, and resulting alerts will not be generated.

## Copyright and trademark notice

Copyright © 2005 LANDesk Software, Ltd. or its affiliated companies. All rights reserved.

LANDesk is either a registered trademark or trademark of LANDesk Software, Ltd. or its affiliated companies in the United States and/or other countries.

\*Other brands and names may be claimed as the property of others.